FACULTY OF TECHNOLOGY

RISK MANAGEMENT FOR UNIVERSITIES IN THE AGE OF CYBERCRIME

Susan Sandell

Industrial Engineering and Management

Master's thesis

April 2021

ABSTRACT

Risk Management for Universities in the Age of Cybercrime

Susan Sandell

University of Oulu, Master's Programme in Industrial Engineering and Management

Supervisor(s) at the university: Kirsi Aaltonen

In a time where there is an increase in online traffic, and needing to have an online presence, education in the risks associated in going on the internet is more important than ever. This study aims to help educate potential companies and individuals to design and implement an effective risk management plan in order to minimize risks when dealing with the uncertainties of the internet. The research problem that this thesis hopes to solve, is how many industries, especially how universities can prepare themselves for potential cyberattacks, as they may have outdated security that does not offer enough protection. Now, most universities are unprepared, and this can potentially be a massive problem when it comes to possible data breaches. Security for universities is the focus of this study, to try and spread awareness and encourage universities to implement a successful plan by looking at both good and bad examples. This study utilizes a variety of research methods, surveys were conducted to gain a widespread insight into how secure people were online, as well as more in-depth interviews were held. The target groups were preferably students, and people around the ages of 18-30. The outcome of this study shows that not all universities are equally prepared when it comes to potential attacks, but with implementing security requirements, this would help provide guidelines and ensure that every industry is protected. When it comes to the university sector, students gave answers that proved they were aware of how to stay safe online, and not fall for scams.

Keywords: Risk management, Cybercrime, Internet Security

FOREWORD

I would like to briefly thank all of those who were involved in helping me complete my master's thesis study.

Firstly, to my advisor who gave her free time to help guide me and arrange interviews for this study, and who was always patient and understanding if something came up. Without her, none of this would have been possible.

I would also like to thank my mom, husband and two pets for their moral support and reminding me to take regular breaks from my work.

Lastly, a thank you to the individuals I interviewed, thank you for your time and your input. For the widespread survey, thank you to the 35 individuals who took a few moments to answer my survey and help with my data collection. Also, I would like to thank a member of the IT staff for their time and information about the University of Oulu's IT security and traffic.

Susan Sandell

TABLE OF CONTENTS

FIGURES

LIST OF ABBREVIATIONS

BBN: Bolt Beranek and Newman Inc

BTX: German based computer Network

CCC: Chaos computer club

C&C: Control servers

Cdc: Cult of dead cow

CRO: Chief Risk officer

CWG: Conflicker working group

ERM: Enterprise risk management

JLA: James Lam and associates

HTML: Hypertext markup language

URI: Uniform resource identifier

HTTP: Hypertext transfer protocol

VPN: Virtual private network

MIT: Massachusetts Institute of Technology

EDT: Electronic disturbance theater

DM: Deutsche marks

DDOS: Distributed denial of service

SSN: Social security number

MRI: Magnetic resonance imaging

Ext: External

DOS: Denial of service

IRC: Internet relay chat

DNS: Domain name system

P2P: Peer to peer

POD: Ping of Death

ICMP: Internet control message protocol

ENISA: European Union agency for network and information security

IOT: Internet of things

1 INTRODUCTION

1.1 Background

In today's world, cyber related crimes are on the rise, due to the incredible amount of confidential information stored on servers that are not secure enough from professional hackers. Once sensitive information is leaked onto the internet, it is nearly impossible to get it back. Leaked records can cost companies millions each year and can lead to loss of trust with their customers, or even in some extreme cases, lawsuits.

Some industries are targeted more than others, due to having more valuable, or rich information in their servers. For example, a hospital would be more desirable to have access to rather than a construction company. This is because hospitals have confidential information of thousands of patients, as well as financial information. In contrast, a construction company may only offer blueprints and information on not even a dozen employees.

Risk management's goal is to help make a company aware of most if not all the potential risks or dangers out there and helps them create an effective strategy that is unique as the company itself. Once the company is aware of the risks out there, and how they will deal with them, should it happen, damage is minimized if not completely avoided.

Hackers unfortunately will keep improving their methods and will always try to breach the most secure systems in order to have bragging rights for accomplishing it. Skills are not even needed in some cases, and certain hacks can be bought online on black-market websites. Hackers are not short of choice when it comes to methods of attacks, whether it be by software or a network of computers they can use to crash the company's entire system.

A system is only as secure as its most novice user, in the same way a chain is only as strong as its weakest link. This means that an internal system, such as an intranet must be kept secure. This is accomplished by educating those who use it by teaching them safe practices on the internet. What could potentially compromise the security of a system could be as simple as a seemingly harmless link clicked in an email that appears to be from someone the recipient knows.

1.2 Research objectives and research questions

This thesis' key concepts are to get the reader to learn more about the history and rise of cybercrime. In addition to this, some cases of attacks and how they were handled, then lastly to educate them on how they can protect themselves before it is too late. The scope of this project covers risk management when it comes to cybercrimes, and focusing on how universities are targeted, mostly due to them being unprepared for any type of cyberattack. Universities were chosen as a focus area, due to me being a student and how I could personally be affected. Due to universities being a more recent target, there is not much information out there gathered in one study as a single piece.

The research question for this thesis is: How prepared are universities when it comes to cyberattacks, as well as how knowledgeable are students and staff when it comes to cyber security

1.3 Structure of the thesis

This thesis covers the history of risk management and the history of technology, as well as the history of the internet and cybercrimes, mainly focusing around the university sector. These sections have a lot of available information online, and the decision was made to focus on key, landmark events that changed the world of risk management and cyber-security.

Data breaches are covered to give the reader more of an idea as to what the differences are. Viruses/malware are separated due to them being different. Many use the words interchangeably, so this will hopefully clear up the confusion.

The top targets as well as a focus on universities as a target offers the reader more information about how safe their information may be and why these targets are possibly popular for attacks. Having a secure university network with thousands of logins a day can prove difficult with implementing effective security, to distinguish genuine user accounts from fraudulent ones.

Response options can help determine what could be the best option for the situation and encourage others to learn more about them before they are needed.

The objective of completing this thesis is to hopefully spread awareness of the rise in cybercrime in businesses, with a focus on Universities since they are the latest victims who are most likely to be unprepared for an attack.

2 LITERATURE REVIEW

2.1 Background of risk management

The goal of risk management can simply be defined as “to minimize unexpected loss”, and “since the future cannot be predicted, at least financial risk can be.” (Crouhy, M, Gdai, D. Mark, R, 2006). The utilization of risk management exists in nearly every field one can think of. In order to have a successful business, the potential risks should be identified early on and plans should be made on how to deal with them.

Risk management has been around as a concept since possibly ancient times. Games where probability is a factor made people think of potential risks while playing. Two famous mathematicians, Pascal and Fermat exchanged many letters in the 1600s discussing the idea of probability. Pascal was well-known for his various dice problems in probability, such as: "When one throws with two dice, how many throws must one be allowed in order to have a better than even chance of getting two sixes at least once?" (Ore, 2017)

Risk management as a concept for insurance even dates back to ancient Babylon, where the first ever laws were written down. These laws were known as the Hammurabi code, named after the king of the same name. These laws were revolutionary and as for insurance it stated: "a debtor did not have to pay off loans if some personal catastrophe made it impossible" (Beattie, 2020)

Risk management as we know it, started after WWII, around 1955 and is most often associated as being an alternative to market insurance. Unfortunately, market insurance was very costly and often only used to protect individuals and companies from losses in the forms of accidents.

This was improved upon by the 1960s, where contingency or possible back-up plans were drafted, and workers could be protected in case of work-related injuries. The difficult aspect of insurance was that it could not anticipate every work accident, therefore it could not cover everything without it being obscenely costly. The alternative at the time was to roll out safety training programs for employees instead of covering them with insurance. (Rhodes, 2015)

Risk management was not actually measured until the 1970's and grew even more popular in the 1980's with the first use of financial management or risk portfolios. This practice was popular with institutions such as banks and insurance companies. (Dione,2013)

Due to the increased probability of risks, a position exists in companies that was started in the 1990's, the role of a CRO, or a chief risk officer. There has been an increasing demand for this employee at companies, and is not an easy position to fill, due to it requiring years of experience and knowledge in risk management, studying the law, accounting and economics.

The first known chief risk officer was James Lam who has now gone on to write several books based off his 20 years of experience in the field of ERM (Enterprise Risk Management) and has worked through his own consulting firm JLA (James Lam and Associates) since 2002. He claims in order to have a successful ERM implementation you need to have "an engaged senior management & board of directors, established policies, systems, and processes that are supported by a strong risk culture. Thirdly, a risk appetite that is well-defined with clear limits/boundaries and robust analytics for intra and inter-risk management. Lastly, risk-return management integration with strategic planning, business processes, performance measurement and incentive compensation." He goes on to add that top-down risk assessment should be done on a regular basis be it quarterly or annually. (Cognos, 2008)

Risk management can be divided up into different types of risk. The first of the risks being, credit risk. Credit risk refers to the item in question may change in quality. This can be a consequence of a borrower's failure to repay a loan, or failure to receive owed interest. This interrupts the cash flow, creating a potential loss for the company. This is why banks only lend money to what they deem as "low risk" lenders, the most likely individuals to pay the loan back. (CNB University, 2020)

In the United States, credit cards are often used in this way, with a scoring system that goes up with good behavior (such as regular use and paying the bills on time). It is not entirely impossible to get a loan with bad credit, but the interest rate may be higher due to the increased risk the firm is taking on.

Market risk deals with the constantly shifting and unpredictable nature of the market. Most market risks are out of an individual's or company's control. Also known as systematic risk, it is known to be unavoidable but can be lessened by diversifying money investments. Such examples include recessions, political conflict and foreign exchange prices fluctuating. (CFI, 2021)

Operational risk covers a wide field, but is a consequence of failed implementation of policies, systems and company activities. The focus in this area are human/employee errors and system failures. All these events have one thing in common: it disrupts the business process and can be costly both in time and money to fix. One example is hiring a less experienced sales team for lower salaries instead of paying higher salaries to individuals with more experience and less likely to make errors. (Segal, 2020)

Legal and regulatory risk refers to changes in legislation that can potentially affect security in companies or even the whole industry. Regardless of impact on the companies, all must follow government regulations. Such examples of these risks include changes in trade policies, like how it is prohibited to invest in Chinese companies/stocks as a foreign company. Even changes as simple as increases in the minimum wage, or changes in sick/vacation days can have a big effect on many companies. (CFI, 2015)

Business risk deals with any exposure a company may get that could lower its profits or potentially lead it to failure. Sometimes this risk is internal, when a company is led by an incompetent leader who makes bad decisions, or it may be external. It's impossible to anticipate every potential risk but can be minimized with a detailed risk management strategy. There are many examples of this, such as competition, employee strikes or a change in the market that had not previously been factored into the strategy.

Strategic risk is defined as "a possible source of loss that might arise from the pursuit of an unsuccessful business plan." There are many places that this can happen, from poor business decisions, failure to adapt to a changing environment or poor allocation of the company's resources. (Dictionary.com, 2020)

Reputation risk is one of the newest additions to the field, based on how the company behaves/reacts can have a negative or positive impact on them. There are many examples of this, but the most famous would probably be from the ride-sharing program called

Uber. In 2018 the company was hit with 56 claims of sexual harassment, but upon further digging also managed to discover minority discrimination and an unethical/hostile working environment. The total amount paid out in settlements over this totaled $20 million and led to many high-level firings in the company. (Bamford, 2019)

In addition to reputation risks, cyber risks are also a newer category when it comes to risk management. A cyber risk is the same thing as a cyber-threat, referring to DOS (denial of service attacks), or any other type of attempt to breach a secure system. Cyber risks can be both malicious or harmless in nature, a malicious threat or harmless threat. (Refsdal, 2015) In other words, cyber risk is the first form of risk management to exist purely to mitigate risks in the digital world. (Britt, 2017)

2.2 Background on internet and technology

It is difficult to pinpoint exactly when the idea of the internet was created, since the idea of it can be traced back to Nikola Tesla back in 1926; “When wireless is perfectly applied the whole earth will be converted into a huge brain, which in fact it is…. We shall be able to communicate with one another instantly, irrespective of distance. Not only this, but through television and telephony we shall see and hear one another as perfectly as though were face to face, despite intervening distances of thousands of miles; and the instruments through which we shall be able to do this will be amazingly simple compared with our present telephone. A man will be able to carry one in his vest pocket.” (Tesla, 1926)

Due to the popularity of the internet, but also the mystery surrounding who exactly should be named with the invention of it, many have taken advantage of the situation and have attempted to take credit for it.

In the 1960s ARPAnet was invented, known as an advanced research projects agency network. This project was funded by the US department of defense and its goal was to be able to connect several computers to a singular "network" connection. This took quite a few years before it worked, but the first message was delivered on October 29, 1969 between computers in northern and Southern California. The message was intended to be "LOGIN" but only the first two letters were sent before the entire network crashed. Even though many would consider this a failure, it was more of a symbolic success, a steppingstone for the future. (Shedden, 2014) (Andrews, 2019) (Lukasik, 2010)

Sir Tim Berners-Lee is credited with inventing the internet as we know it today, but in fact he is credited with several inventions such as HTML (hypertext markup language), URI (uniform resource identifier), and lastly HTTP (hypertext transfer protocol). With the combination of these being utilized, the first web page went up in 1990 and the public had access a year later. Instead of limiting control of this new space, the creator decided for it to truly reach its maximum potential it should be completely free and widely available to use. (Andrews, 2019) (Mcpherson, 2009)

In 1994 W3C was founded, with Tim Berners-Lee as the founder. The world wide web consortium's main purpose was to create standards or guidelines for the internet. The main guidelines are as follows:

1. Decentralized structure: no one owns or controls the internet. Users are free to post whatever they want without censorship and without needing permission from a higher authority. No one person or group should possess a "kill-switch" and users should not be under surveillance or any monitoring. This is an issue in current days, with many companies selling user's data and many countries censoring the internet.

2. Non-discrimination: this is otherwise known as net neutrality. Every individual should have an equal connection to the internet. Unfortunately, today this is also an issue, with many companies attempting to throttle the internet and introducing data limits.

3. Bottom-up design: the code needed to create things on the internet is widely available and anyone can figure out how to create a website.

4. Universality: all the computers connected to the internet around the world need to speak the same "language" in order to communicate with each other.

5. Consensus: every one that uses the internet should have a say about what standards the internet should adopt, making it fully transparent.

These guidelines give the internet an open feeling where people of different cultures and ideas can communicate with each other in a common place and bring people together. (World wide web foundation, 2012)

In the year 2005 the total world population was 6.5 billion, and out of that total, 958 million users were on the internet. Most of the users were in North America with roughly 68% of its population online or 223 million. Oceania (islands based in Central and South Pacific Ocean) ranks second place with 49.2% of the population, 16 million and Europe is third with 36.8%, 269 million users. (Argaez, 2005)

World regions	Internet users, 2000	Internet users 2005	Growth	% of pop. 2005
North America	108,096,800	223,392,807	106.70%	68%
Oceania	7,619,500	16,448,966	115.90%	49.20%
Europe	103,096,093	269,036,096	161%	36.80%
Latin America &Caribbean	18,068,919	68,130,804	277%	12.50%
Asia	114,303,000	323,756,956	183%	8.90%
Middle East	5,284,800	21,770,700	311.90%	8.30%
Africa	4,514,400	16,174,600	258.30%	1.80%
Total world	360,983,512	938,710,929	160%	14.60%

Figure 1 Internet Growth Stats (adopted from Argaez)

At this current year, 2020 the population stands at 7.74 billion people, and the users of the internet have grown to over 4.3 billion. This is very impressive, since from 2000 to 2005 the rate of growth in internet users was estimated at about 5%. Back in 2005 with 49.2% of the population using the internet, currently it stands at 56%, or roughly 6 out of every 10 people. Originally North America was the top country when it came to users on the internet, and only 8% of the population in Asia was using the internet.

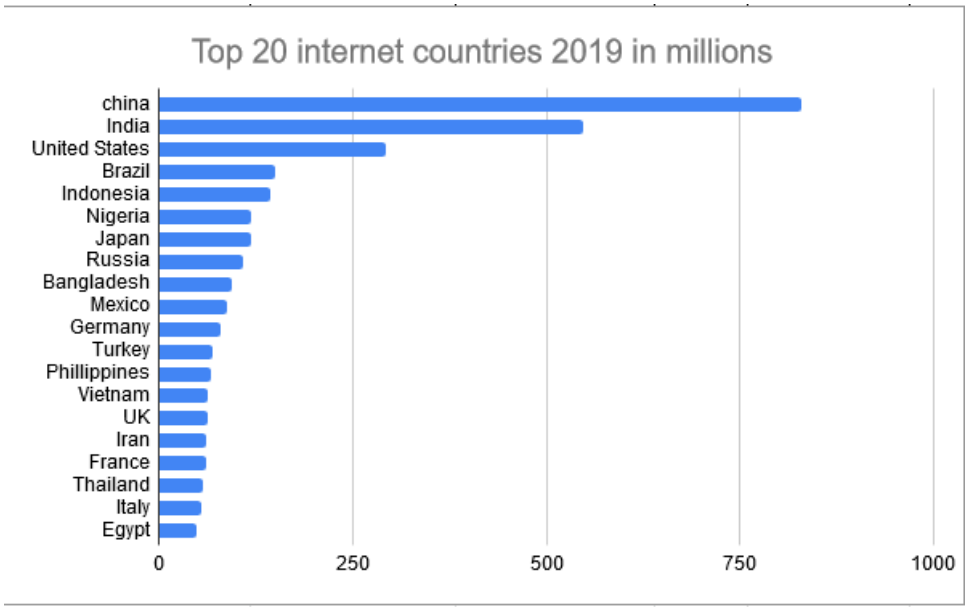


Figure 2 Top 20 internet countries (adopted by Miniwatts, 2019)

This graph from 2019 showing the number of internet users per country tells a different story. Just China alone accounts for 829 million users, and North America is in third place with 292 million. Another interesting thing to note is that many of the other countries or regions on this list were not even on the list in 2005. This shows how in just 14 years how quickly the internet is being adopted.

Out of the 4.3 billion unique users on the internet, 3.9 billion of them are mobile users, using their devices an average of 6 hours each day. Users divide time between social media and communications, various other applications available, streaming content, or accessing the over 1.7 billion websites available online.(Clement, 2020) (Llewellyn, 2019)

Unfortunately, it is impossible to predict the future with complete accuracy, but by using past data to create projections, it can provide estimates for the future. How many people will have access to the internet in 2030? Cybercrime magazine estimates that in 10 years there will be 7.5 billion people online out of a population of 8.5 billion. This growth is based on 2016's 2 billion users and jump to 2018's 3.8 billion users. (Morgan, 2019)

The internet's creator is more than happy with just how much of society he has managed to shape through his invention, he has spent most of his life trying to maintain the integrity

of it, and that it is not used in corrupt ways. Years ago, in the beginning days of the internet he never imagined it could be used to win elections by targeted marketing or to listen to people via such technology as Alexa.

He began plans back in 2016 to launch another similar web program called solid, which is short for socially linked data. On this program, users fundamental rights would be able to be protected, since it appears that the internet in its current form has gone against all the founding rules set back in 1994. He believed this failure was years in the making, users slowly signed more and more of their rights away by accepting various types of agreements made by big companies such as Facebook, Google and Amazon. These companies have been getting in trouble legally when users discovered that their private information was being used for data collection, and devices were capable of recording conversations without the individuals being aware.

Solid would be a re-decentralized web service with a small group of well-trusted web developers. He is trying to act fast with this, because the internet is growing exponentially by gaining users as well as their confidential information. (Brooker, 2018)

Currently, the solid company websites offer frequent updates as well as free individual internet “pods”, personal online data store, where users can run their own servers unsecured at their own risk if they have the know-how. There are also active forums on the website, where developers can build applications and people Who are new to solid can find useful information and connect with others. Currently the website is looking for users to test the service, content creators to make tutorials, security experts to find vulnerabilities in the system, packagers to help make it easier to distribute, then lastly; members to join the community and spread the word. (Solid project, 2020) (Sambra, 2016)

This new form of internet will hopefully take off, because with the way the current internet is going, many are not happy. The spread of fake news, and clickbait headlines to draw in clicks to their pages help companies earn money, but often lead to the spread of misinformation and panic. Each day users' privacy decreases and security/monitoring seem to increase. Users are unable to remain anonymous on the internet.

A famous book, by the name of 1984 by George Orwell warns users about how easily news can be distorted, using words like “doublethink” or “newspeak” which has formed its own term in the real world: “doublespeak”. This process involves the government's use of words to distort reality. Fake news is one of the newer forms of this, and one of the most upsetting ones. In a world that is connected, real news can travel fast, but so can fake news. In a market where hundreds if not thousands of articles are published daily, it is becoming increasingly difficult to discern what is real and what is not. (Goering, 2018)

Even applications that are free and are a benefit to you, cannot be as harmless as they seem. For example, Hola, a free plugin for browsers offers users to watch content that isn’t available in your own country, by making your computer appear to be in a different country, via changing your IP address, otherwise known as a VPN or virtual private network. This may initially seem to be a good thing, but in fact the company was selling users extra bandwidth that was purchasable in bulk. This eventually created a botnet of about 9 million. Some users have panicked at the thought of someone using their internet, and what they used it for. For example, if someone were to access an illegal website, or to do something simply illegal, the crime would be traced back to them instead of the guilty party. The actual guilty person would most likely get away with it, due to the high amount of user data in the system. (Vincent, 2015)

It may be difficult to stay positive about the current state of the internet, but it helps to stay informed and to follow the news. Lastly, it is also important as to what data you put online. Companies seem to have an unending appetite when it comes to user data, since they want to find better ways to market relevant items to you.

2.3 Origins on the rise in hacking and cyber attacks

Hacking is defined as "gaining illegal access to a computer, network or system", and cyber-attack is very similarly defined "gaining illegal access to a computer or network system for the purpose of causing harm or damage" by the 2020 Merriam Webster dictionary. The term cybercrime is defined as “criminal activity done using computers and the internet. This includes anything from downloading illegal music files to stealing millions of dollars from online bank accounts. Cybercrime also includes non-monetary offenses such as creating and distributing viruses on other computers or posting confidential business information on the internet.” (Christensson, 2006) From this, one

can draw the conclusion that hacking does not always have bad intentions, but cyber-attacks do. The differences between these two will be discussed more in depth later on.

It seems like an impossible concept to think that the first incident of cybercrime occurred way back in 1834, before the internet as we know it was created, it even predates cars being invented by 50 years. This may seem to surely be false, but France had managed to set up a sophisticated telegraph 'network' system that had been in use since the 1790's and was only allowed to be used by the government. The hack was also accomplished by two brothers, known as the Blanc brothers who observed the movements of the mail. The brothers bribed a telegraph operator and got them to send errors in the expected routine messages. This went on until 1836, unnoticed for 2 years and the only reason the brothers were caught is because the bribed operator became ill and asked a friend to take his place in the scheme. Since it was the first crime of its kind, there were no laws against it, so the brothers got away with it. (Standage, 2013)

There have been many cybercrimes and various hackers throughout history, many come off as doing it for their own benefits, however, there have been ethical hackers as well. The first known ethical hacker goes by the name Rene Carmille, a member of the resistance against Nazis in France. He was one of the first to introduce national registers for census purposes. Rene was aware of how the Nazis punch card machines worked, and how they were used to hunt down Jewish people. He then decided to plan; hack into his own system and no matter what the Nazis wrote in the file, it did not label them as Jewish. (Nycyk, 2020)

Rene got away with this for 2 whole years, saving thousands of lives. He claimed he did not know why the machines were not working, which they believed at first. Sadly, once the Nazis discovered his lies and sent him to a concentration camp where he was tortured and killed. (Wills, 2017)

In 1962 MIT, (Massachusetts Institute of Technology) set up the first password-protected computer that students were able to access. Since the number of available computers was extremely limited, a 4 hours per week time limit was implemented for each student account.

Alan Scherr was an MIT student, who wanted more time on the computers because it was not enough to complete his work. He fortunately had a higher level of access than most students, so it made it easy to enter code to zero out his usage time. In 1966, he finished his research and with that, he then lost the high level of access. He still wanted to figure out a way to get more time on the computers each week, so he got to work on finding a way. He discovered that if you made a print request, there were no security limits in what could or could not be printed. This was exploited to print out a list of every one's usernames and passwords. To ensure that this hack would not be placed on him, he gave out lists to a select group of people and managed to get away with it. The inventor of the password, Fernando Corbató was impressed with this, but it also showed how very flawed some systems could be. The original use of the password was not intended for security, but rather differentiating files, he stated. This misunderstanding could have helped companies create better security measures to prevent future attacks. (Kalat, 2018)

Before the word “hacker” was coined, these individuals went by another name. Before computer hacking became a widespread problem, phones were the targets in the 1980’s. These early, simple phones were easily manipulated into making free long distance phone calls, if you had a device called a blue box. The device made it seem that the call was coming from an operator, which bypassed systems and switches. This group of people called themselves phreaks. The word comes from the act of phreaking, and includes the processes of exploration, experimenting and study of telecommunication systems. This practice lost popularity when companies started offering free calling, including long-distance, and with the adoption of cable modems also came more advanced security measures.(Baraniuk,2013)

Phreaks had even discovered that there was a way to add multiple lines, like a conference call set-up. This was called the "2111 conference". Complex understanding of phone systems and how to add/remove individuals was needed to accomplish this and was surprisingly popular with blind teenagers. These teenagers felt lonely and were able to memorize numbers and recognize various tones the phone made. (Donovan, 2016)

In the year 1981, Ian Murphy was the first person who was convicted for cybercrimes. He was responsible for hacking into AT&T’s network to change the clock to charge cheaper rates. Although he never set foot in an actual prison, he was sentenced to 1000 years of community service as well as 2.5 years of probation. This was a landmark case, however, since previous crimes went unpunished due to no relevant laws being put in

place to convict individuals guilty of digital crimes. (Delio, 2001) Another notable hacker was Max Butler, a man who in 2006 wanted to take over the black market for himself, so he could hoard all the profits. Through the years, he was always having his eye on just how profitable the black market was, and how rich it could make him. He knew that this would not be easy, so he slowly improved his skills with easier hacks that ramped up in difficulty for 20 years.

Before this, he had served 18 months in 2001 for breaking into federal sites to fix their security, in addition to installing a backdoor for himself. The government stated that Max caused $60 000 (equal to $89 000 in 2021) in damage, based on time needed for the companies to recover from the attacks. Max has a very long rap sheet of crimes and made quite a bit of profit off his illegal activities in the past. (Poulson, 2001)

He completed this by stuffing his small apartment in San Francisco with servers in addition to laptops to attempt this mammoth feat. He began his attack and took down the carder or marketplace sites used to buy and sell identities then he drained them of all their information. This information included users' logins, passwords and emails and then wiped the site clean.

This was very intense, sensitive work, so after working for 2 days without break, he would sleep for only a few hours at a time. He knew that this was not a time for rest, and that he needed to be ready for anything. Max then sent emails to all the users stating that they were all now members of his site, in doing this he had collected several thousands of users who were scattered over dozens of websites to only one, his website: cardersmarket.com. Some good did come with this attack though, he made the website secure and reliable unlike the previous competitors' sites who were sketchy at best. (Poulson, 2011)

Although things went well for a period, this did not last. He bragged about how he accomplished this and how it made him smarter than everyone, and this caught the attention of various law enforcement offices. Butler thought he was one step ahead of them by announcing his retirement and how someone else would be taking over the site, but this was not completely true, he simply retired his old account and started up with another one. Due to the delicate nature of this, the FBI was not able to catch him until 2005 after catching an accomplice of his, Christopher Aragon. When Butler was apprehended, an officer stated that he had about 1 million credit card numbers on his hard

drive. This was a huge surprise that he was holding on to all these numbers since it could equal about $500 million. Although Max Butler is not the first person to be arrested for cybercrime, he is the first person to be given a life sentence for it. (Poulson, 2008)

The last hacker is impressive due to his young age, Jonathan James who was only 15 years old when he managed to access the US Department of Defense and was able to even install a backdoor for access later. In doing this he was able to read thousands of private emails, even ones containing usernames and passwords for military computers. Initially he cost NASA $41,000 from stealing software that left the systems unusable for weeks. (Emma, 2020) This software "supported the international space station's physical environment, including control of the temperature and humidity of the living space." Since he was only 15, he was given a 6-month sentence, whereas if he were an adult, it would most likely have been at least 10 years. Attorney General Janet Reno and lawyer Guy Lewis issued statements calling for a tougher stance on cybercrime for those underage. If a criminal is underage, it is most likely seen as a prank, whereas an adult breaking the law is seen as a criminal in need of incarceration.

Sadly, in 2008 he committed suicide after accused of being an accomplice in a massive 2007 credit card hack, of which he claimed to be innocent. (Stout, 2000). These various hackers have made their mark on history for their crimes, despite how different they are in task and in motive. These individuals have shaped laws and help improve security infrastructure over time, making sites required to follow security laws and regulations to protect its users.

2.4 A Background on hacktivists

Hacktivists, or hacker activists are a new type of activism in the 21st century. Humans have always felt the need to stand up for what they felt was right and oppose oppression. This ranges historically from the United States fighting for independence from Britain, with the cry "no taxation without representation", wanting to abolish slavery, women fighting for the right to vote, and equality for all. All these issues are important, and we as a collective owe our ancestors our gratitude for shaping the world into a fairer, better place for all. (BBC Teach, 2016)

Due to the increase in popularity of the internet, it is no surprise that activism has spread digitally. News can spread faster than ever, and people are now able to be more informed

about the events going on around the world despite being thousands of miles apart, in an instant.

This is a double-edged sword, since it can work to spread positivity, but it can also spread negativity. Hacking has become popular due to its low cost to set up, and how relatively easy it is to carry out. Individuals are not limited geographically, and you can stage an attack anywhere in the world.

The word, hacktivism was coined in the year 1996 by a member called Omega, from the hacking group that went by the name the cult of dead cow, or cDc for short. Their motive was to "leverage technology to advance human rights and protect the free flow of information." The (Mccormick, 2013) The group has been known to partner with others to help hack and take down government networks. One such example is helping take down Chinese government websites with Hong Kong activists. China is a controversial country that does not have a good record with various types of human rights and is said to be a corrupt country altogether.

Nowadays the cDc is not as powerful as it once was, due to people branching out to form different groups, most likely because of differences of opinion. Hacktivism is one of the bigger branches and is probably known for defending users' human rights and political rights to freedom of opinion and expression on the internet.

In the late 1990's a group of activists went by the name Electronic Disturbance Theater or EDT for short. This New York based group created the concept of virtual sit-ins via software of their own creation called flood net. This tool refreshed the targeted websites, so it did not have to be done manually. The group had an agreement to not be anonymous, since they would not have that luxury when protesting in public.

Anonymous is arguably the most famous hacktivist group out there, and this is likely from their viral videos that have an ominous tone to them with various messages they want to deliver. No one knows exactly how big this group is, but they have thousands of members from all over the globe.

This group was created on a website, called 4chan in 2003. The website originally was meant to have users post and share interesting content, in addition to chatting and making friends with the same interests as you. The interesting thing about this website was, if you

did not fill in a name for your posts, it got filled in as “anonymous” for you, allowing the user to hide their identity. These anonymous users could post anything they wanted, without it being traceable back to them. Using this, a group of pranksters formed who tried to one-up each other as a part of a competition and built up until it reached coordinated internet attacks.

The first major targeted attack was towards the church of scientology of all things, in the year 2008. The reason for this attack was odd, but they felt justified in their actions. The tv talk show Oprah posted a video clip on YouTube where she was giving an interview with the movie actor, Tom Cruise. In the clip he seemed to be laughing hysterically, jumping on the couch and seems unable to sit still. The reason for this was, he claimed because he was happy and in love. (Toma, 2018) (Goode, 2015) (YouTube, 2008) Tom Cruise loses his mind on Oprah This came off as quite odd, since no other interviews typically go like this. As with most things that are humorous on the internet, it was shared all over its various websites and was watched by thousands of people. Later, it was even in Scary movie 4, known for its parodies on pop culture.

The church was greatly displeased with how the spokesperson of scientology was openly being mocked online and having some of the negativity reaching the church. The church then decided to have the videos on YouTube removed due to “copyright infringement”. There is no doubt in that this was an abuse of power on their part, so anonymous decided to act on what they deemed a violation of human speech.

The church was about to be attacked and have all their dark secrets revealed to the public, courtesy of the hacktivist group. Anonymous made various statements about how harmful the religion is, and how hard if not impossible they make it for members who want to leave. This prompted many to leave the religion entirely and cut all ties with it.

Anonymous even managed to get people to protest internationally in person outside the centers over the globe, with signs, but with protecting their identities hidden under Guy Fawkes masks, like the one worn in the movie V for Vendetta (2006), a movie about a dystopian totalitarian future in the UK where a terrorist known only as V fights to bring down the oppressive government. The movie reaches its conclusion with having achieved his goals, and even manages to have people dawn the mask and go to the streets to join in in protesting. (Infosec, 2011)

The parallels of this movie lie with Guy Fawkes, who also had planned on blowing up parliament and killing members of the government back in 1605 due to being unhappy with a protestant king and wanted to replace him with a catholic one. This was also referred to as the gunpowder plot. Unfortunately, unlike in the movie, Guy Fawkes and company's attempt to assassinate King James I. The plot failed due to a leaked letter, and after a brief battle, the surviving participants, including Fawkes were hanged and killed. (Sharpe, 2018)

Since then, the night of November 5th has been celebrated as Guy Fawkes night, or bonfire night more recently. Kids make and sometimes sell effigies of Guy Fawkes, or other criminals out of newspaper, clothes and even masks to burn. (Greenspan, 2012)

The link between the masks and the movie lies in that the times anonymous uses them is to protest politicians, banks and commitment towards protesting a shared cause. Unlike the movie, the organization of anonymous exists worldwide and protests regardless of geographical location. Due to the lack of consistency in protests though, some being peaceful and others being violent has led to the masks having a potentially negative radical association.

The country of Saudi Arabia has even banned the importing of any V masks due to them "instilling a culture of violence and extremism" (2013) according to the Saudi Ministry of Islamic Affairs. Besides the importing of masks, all masks already for sale in the country would be confiscated and destroyed. Saudi Arabia was the first country to specifically ban these masks. (Stuster, 2013) No other countries have joined in on specifically banning the Guy Fawkes mask, but other countries have been banning any mask wearing in general for protests that prevent them from being identified.

There are other groups of hacktivists, but unfortunately none of them have been able to gain as much notoriety as anonymous has, despite there being groups that had already formed before anonymous was created. One such group, known as CCC, or the chaos computer club, a European hacking community was founded in 1981 in Germany. The founder, known as Wau Holland founded this group with the belief that computers could be used for human rights. In 1987, they made the news with the first ever case of cyber-espionage. CCC breached the US government, as well as other corporate computer systems and were selling the source code to the KGB. (Middleton, 2017)

This group of people had anticipated the popularity that IT would play in daily life, and for their next attack the had hacked into a Germany computer network, known as BTX in 1984. The company had boasted publicly about their great security in the days before the incident. The group managed to retrieve 134 000 in DM's (Deutsche marks, a currency used in West-Germany from 1948-1990), and then returned it publicly the next day.

Wau Holland had many admirers, who appreciated his involvement in activism and standing up for human rights. Despite the leader's passing in 2001, the collective group still carries on in his honor, and have even been able to make headlines fairly recently with showing that it is possible to trick an iPhone 5s' fingerprint scanner into unlocking from a photograph of a fingerprint. (Kettman, 2001)

Within the hacktivist collective, there are groups who use their hacking knowledge to harm or at the very least to inconvenience others and the other side of the coin features those who want to use their knowledge for good. These opposites are known as black hat hackers, and white hat hackers. Black hat hackers, try to cause as much chaos and harm as possible. One example of black hat hackers would be a group known as lizard squad. They are most known for their first attacks, that disrupted all gaming services via DDOS attacks in the year 2014.

A widely known game, League of legends was targeted in August of 2014, as well as the PlayStation network. Then again on Christmas, to prevent people from being able to play their games, the group attacked both the PlayStation and Xbox networks. The attack was withdrawn when they were offered free lifetime accounts on an online encrypted file hosting service, called Mega. (Fung, 2014)

The group does not limit their attacks to taking place online, around the same time that the attacks took place, the group tweeted out a bomb scare. This forced American Airlines to make an emergency landing and evacuate the passengers, including the possible target, the president of Sony online entertainment, John Smedley. Many have claimed that certain attacks had been carried out under the name of lizard squad but have then been disproven by other members of the group. One of the members who was 17 years old came forward and was convicted of 50 700 charges of computer related crimes but will only serve a two-year suspended sentence and will not need to serve time in jail. (Tassi, 2015)

Unfortunately, it is impossible to write about every hacker group out there, as there are dozens that are publicly known as well as even more that operate secretively. Of these groups, several have officially disbanded, and members have found their ways into other groups.

With the rise of hacktivists, countries have needed to work together in order to prosecute the guilty individuals involved in the attacks, since most do not originate from the country itself. This has proven difficult because if the country does not have a mutual assistance agreement, they may refuse to help bring the individual to justice. One example would be in 2007 when Russian hacktivists targeted Estonia with cyber-attacks that greatly disrupted their whole country in order to protest the moving of a Soviet war memorial. The attack was traced back to Russia, and Estonia demanded that the guilty individuals be punished, but Russia refused, explaining that they did not have a mutual legal assistance treaty. (Traynor, 2007)

Since most cyber-attacks fall below an official use of force, for most countries, it is almost impossible to arrest groups currently. In the future, as these digital attacks become more commonplace, it would be highly recommended to pass certain laws that would make it easier to prosecute these harmful acts. (Denning, 2015) It is unclear what will occur in the future when it comes to hacktivism, but often ebbs and flows, like a tide in a reaction to current world events. With the current state of the world, regarding the highly controversial 2020 United States presidential election and the coronavirus pandemic, it is most likely again on the rise.

2.5 Top industry targets

Before going into what industries are targeted the most, one must understand why certain industries are targeted. Money was originally a target, which meant banks, but with increasingly strict international security guidelines, it has become almost impossible to steal from them.

Hackers in the modern days have discovered that information can sell for more money and once into the system they are potentially able to access hundreds or thousands of people's personal details. In the United States, if someone discovers your social security number, they can potentially steal your identity and it can take years to get it back. Credit

cards can be started in your name, loans can be taken out and even in some cases, wrongful incarceration.

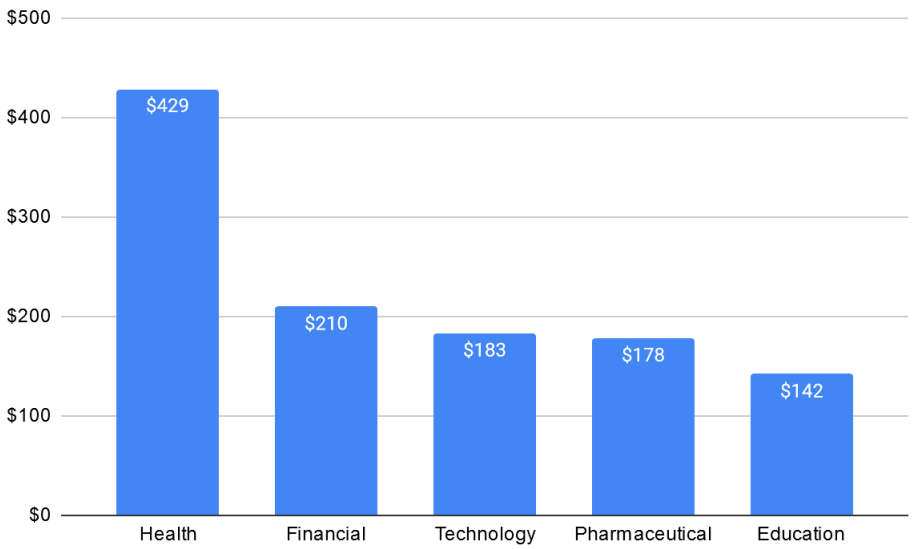


Figure 3 Average cost per record (adopted by Ponemon institute 2019)

Above shows a graph that states the cost of the average record compromised due to a breach. Health is the highest costing one, due to the rich amount of information they have on file, costing an average of $429 per record. Following that is the financial sector at $210, nearly half of the cost of a health breach. Technology and pharma are even lower at $183 and $178. Education, at the year this was recorded, was one of the lower ones, at $142 per breach. In the future, it is expected to rise. (Ponemon Institute, 2019)

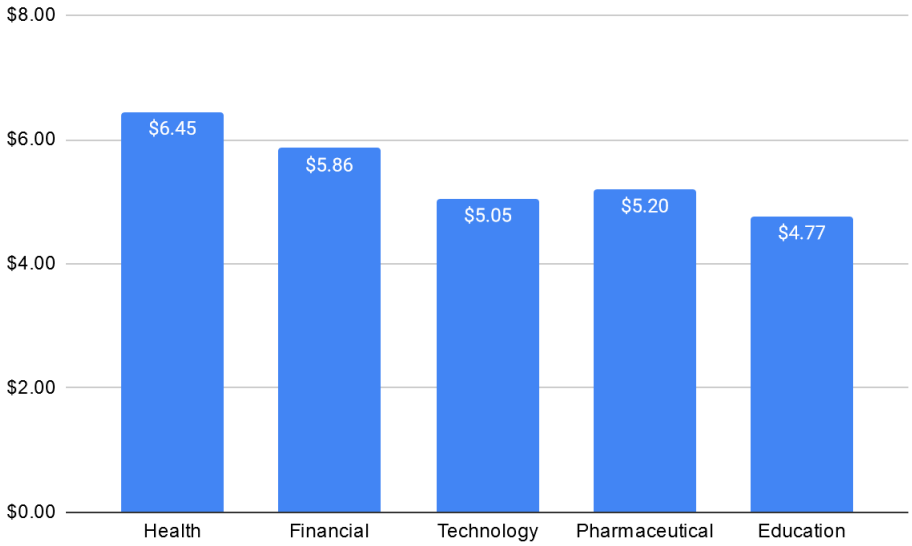


Figure 4 Average cost of data breach per industry (adopted by Ponemon institute 2019)

This graph shows the average cost of a data breach per industry and is measured in millions of $. The health sector is still the most expensive, at $6.45 million. All the sectors seem closer together in amounts, with not as great of a price difference as shown in the previous graph. However, education is one of the lowest industries on this chart, still. It is possible, that the reason due to the lower cost, is that students probably are unaware of data breaches and upper education facilities are not hurt by loss in reputation as much as a financial or health institution. Another potential variable is the number of customers each industry receives.

Government agencies are a very rich target for hackers, due to them storing private information on millions of people in one place. Hacks have ranged in size, from targeting the state of Texas in 2011, affecting 3.5 million people's tax information up to in 2015, where 191 million were affected by the US voter database being breached.

The biggest government breach to date, was discovered by a man named Chris Vickery who works as an Up Guard cyber risk analyst stumbled upon these records by accident. Apparently, the records were online due to an "incorrectly configured database". The data included: names, addresses, phone numbers, birth dates, party preferences, and emails. (Finkle, 2015)

The financial sector has been under attack for almost if it has existed. First it started off with theft via bank robberies and fraud, but the attacks have changed with the times of the digital age and can be traced back as far as 2007. With attacks and breaches of customer information so early on though, the industry has created stricter security and standards. Unfortunately, the attacks keep coming and show no sign of stopping.

In financial sector attacks, there are two different “costs” associated with it. There are direct costs that are easier to calculate, such as leaked records and stolen money, but there is more than that to consider. Indirect costs must also be included, such as loss of customer trust, leading them to do their business elsewhere. PR, public relations will also have to work on strategies to regain customers and their trust, to minimize the loss for the company. (Tariq, 2018)

The worst hack so far to occur in the financial sector would be the Equifax hack in 2015. Equifax is one of three of the largest credit reporting agencies in the states. The attackers had access to over 143 million customers' private information, such as driver's license numbers and social security numbers. The company got in trouble, since this was the worst hack yet in a series of hacks, and previous hacks had not prompted them to upgrade their security measures. (Bernard, 2017)

Since the attack, Equifax has reached a settlement of $7.75 million to affected customers and have reported to have lost $1.35 billion in losses. A part of the agreement also states that the company must upgrade their security, pledging $25 million on what is planned to be a two-year project. (Coble, 2020) (Wang, 2018)

The healthcare industry deals with billions of patients worldwide, and not many people think to ask about how secure their personal information is. These industries collect all sorts of patient data, such as social security or identification numbers, and financial information which are in high demand on the black market, as stated earlier on in this thesis. Some hackers have even had success in attempting to sell back patient information, such was the case for Hancock regional hospital in 2018. The hospital stated it felt like they had no choice, due to the timing of the attack, at the peak of cold and flu season. The hospital paid $55 000 in bitcoin, and none of the records appeared to have been stolen. (Lovelace jr, 2018).

In addition to leaking confidential records, hackers can also connect to some medical equipment, such as pacemakers. This is frightening, because unsecured medical devices, especially pacemakers are keeping these individuals alive, and if it were to be compromised, a patient may die. (Wellington, 2013)

Due to hospitals employing a significant amount of people, some hackers have even managed to hack into payroll systems to change where salaries go, so they themselves are getting the money, instead of the medical staff member who is employed. (Wright, 2016)

More recently and locally, an attack has happened in Finland. Thousands of psychotherapy patients from a private practice, called Vastaamo, who have 25 centers spread over Finland have had their records stolen. Some records have been leaked, to show proof and many patients have been receiving ransom-like emails, demanding a fee of €200 to prevent the private discussions with their therapist being made public. This attack preys on vulnerable people, mostly underage who may be desperate enough to pay to get their records back due to the stigma surrounding mental health.

Although the investigation is still ongoing, many say that the attack could have been avoided if Vastaamo had been using better encryption software. This will hopefully be a wake-up call for all industries in Finland dealing with sensitive information to upgrade security before it is too late. (Yle, 2020)

2.6 Study of universities as a current target

One unexpected target that is quickly gaining popularity are universities. This is most likely due to their rich personal information about students and staff that is not stored in secure ways. Even if you are not a student, and just merely applied to the school, your information could be at risk.

Staff and student emails are initially the target and enable the hacker to send fake urgent emails to them, and it is hard to determine who is illegally gaining access into the system due to the high volume of logins on various devices daily.

In many universities there are also well-funded research projects that are desirable for hackers to access and then sell online. Some of the most sought-after projects are ones

that are funded by the DOD, department of defense or military. Due to the high level of collaboration and communication, the security level is minimal at best, making it incredibly easy to gain access to. These attacks that are targeted at the researchers are called “spear phishing”, and its goals are to pose as another university or researcher via email to gain information, money or to gain internal access via malware.

In the scientific article, called “phishing in a university community; two large scale phishing experiments focus on the vulnerability the end users present in a university system. This experiment took place in 2010 at AUS, (the American University of Sharjah) that had at the time of conducting the experiment; an academic population of 10 568. The experiment involved sending spoofed emails that appeared to be from the IT department. The email asked individuals to fill out forms in order to reset their passwords on a fake website that was set-up for the sake.

After 10 days of running the experiment, nearly 9% fell for the first phishing attack, and provided their account and password. This 9% consisted of: 9% of the student population, and 5% of the staff population, of which 485 were female and 469 were male. The biggest groups of students that fell for this scam, were seniors at 35%, followed by freshmen at 29%. The lowest group would be the juniors at 16%.

Fortunately, during the 10-day period, several university members contacted the IT department, and after 2 hours they were able to send out a warning email to prevent more people from giving their details out. This was effective, but unfortunately, nearly 1% of the victims gave their information after this email was sent out, appearing to have never read it or ignored the email entirely.

A second experiment was held, where an email appearing to be from an independent third-party research group asked for an individual's personal information, but luckily this email was less effective in gaining confidential information. 224 individuals (220 students and 4 staff), roughly 2% of the school’s population fell for this. Of these 220 people, 86 were female and 134 were male, 4 were unable to be identified.

This study did not seem to find a link based on age or gender, since the oldest and youngest groups of students both fell for it the most. Gender also seems to be irrelevant, since more females fell for the first phishing attack, but more males fell for the second

attack. Although no connection was found, education in how to keep your information secure, as well as paying attention to emails from the IT staff are important. An example of a good, quick response would be the Regis University attack in 2019. This school received a ransomware phishing scam email that targeted students and staff and was believed to originate outside the US. The cyber-attack happened before school started on August 18th. The school responded by disconnecting all Wi-Fi in the school, as well as all internet services offered. In doing this it prevented the attack from spreading and infecting more systems and to start on their official response plan. This left students unable to pay their tuitions, to see exams as well as their school schedules, but a temporary website was put up to inform students of the progress updates. Pretty much all the data was restored on the 20th, and systems were back to normal on the 26th, just in time for classes to start. (McKenzie, 2019)

An example of what can happen if you do not have any plan in place, or any backups of your websites, etc. would have to be what happened to the Baltimore city government. Their systems were taken hostage, leaving them unable to complete many services, such as billing residents. The hackers originally wanted $76 000, but even if you pay, it does not guarantee that you will get what you want back. Also, if you pay it can increase the likelihood of you getting targeted again in the future. So, paying was not an option, said the mayor. Instead, they went offline for over 6 weeks and rebuilt all their systems. This cost the city more than $18 million. (Eiten, 2019)

Universities should try to take initiative and put plans in place to educate students and staff about potential fake emails floating around, and to not click links in emails. If an email comes through that looks urgent, tell them to investigate the email thoroughly before believing it to be true. If they are also afraid that an email may be a scam, to tell the IT department so they can investigate suspicious looking emails and can warn others.

2.7 Data breaches

Data breaches, otherwise known as the illegal under the radar way of gaining access to normally confidential data without permission, has been going on since the 1980’s. This is before computers were commonplace and data was being stored online. In 1984 TRW, the largest credit card company in the United States had its password leaked onto an electronic bulletin board that was available via phone. 90 million individuals' credit histories were made public, which in doing so made their name, address, date of birth and

social security numbers public as well. With this information, anyone could open credit cards while pretending to be the individuals and spend upwards of the credit card's limit. Once the company became aware of this incident, files had been accessible for a month and nothing was charged. TRW got extremely lucky in this case, as well as the 90 million individuals whose data became public, it could have potentially cost the company millions in damages despite the lengthy response time. (Diamond, 1984)

Unfortunately, data breaches have not been officially recorded until 2005, when the government-run non-profit Privacy Rights Clearinghouse began documenting significant data breaches. On their website, individuals can access a free document that shows a history, as well as sign up for updates for notifications on future breaches. (Privacy rights clearinghouse, 2020)

Hacking and illegally gaining access in the 2010's has been made easier with the widespread adoption of computers, the internet and most importantly, cloud storage. Technology is more connected than ever, nowadays and it could just take one password breach for the hacker to gain access to all your sensitive information. Many accounts, for example, have linked credit card numbers and in which have your address, social security number and full name. Data is high in value in the dark web markets, for this very reason.

The most dangerous aspect of data breaches is that information can spread quickly to multiple people, and the companies who store your data may not be aware that a breach is even happening if the hackers are able to go under the radar for long periods of time. Large companies can take time to respond, as well as notifying the public about the breach. Companies can also deem a breach "insignificant" and not go into much detail, if any at all. (Trend Micro, 2017)

Admitting failure is a difficult thing for companies to do, since it is most likely that they will lose the customers trust and therefore, their business with the affected company. According to the Ponemon Institute, a study conducted in 2019 calculated the costs associated with a data breach. To calculate the costs, several factors have to be included. The ABC, or activity-based costing method is used, with four factors affecting the cost of the breach.

1. Detection and escalation: what are used to discover the breach (ex: forensic accounting)

2. Notification costs: The process of notifying those affected individuals of the compromised data in the company. This can be done in person, by email or letter.

3. Post data breach response: The method established to help those affected and potential reparation costs, such as legal fees.

4. Lost business cost: potential lost customers and lost business due to loss in trust or company downtime.

The 2019 study took place in 16 different countries, and 86 companies in total. This study has been occurring annually since 2005, thus making it easier to compare and track the average costs of data breaches each year. The trend of the graph shows that data breaches are on the rise, and cost companies millions of dollars each year.

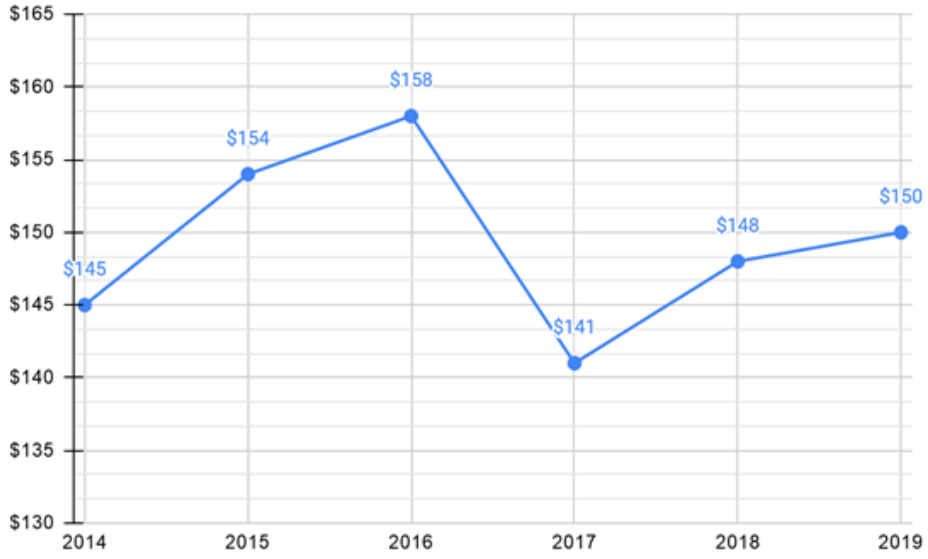


Figure 5 Cost of a compromised record (adopted by Ponemon institute 2019)

The graph above, tracks the average cost of a single compromised record for a company. As shown in the chart, records reached a record high price at $158 in the year 2016 and

dipped at its lowest cost of $141 the next year in 2017. The following years show a slow increase in price, ending with 2019 at $150 per record.

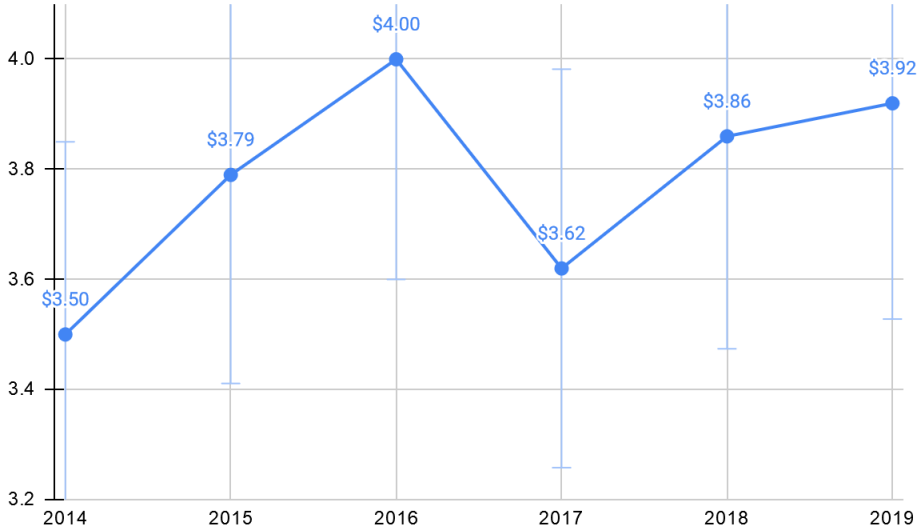


Figure 6 How much is globally spent on data breaches (adopted by Ponemon institute 2019)

The chart above shows globally how much is spent in total on data breaches. The costs are measured in $ millions. As you can see, since the year 2017 the costs have gone up and are continuing an upward trend, possibly surpassing the record high, of $4 million. (Ponemon institute, 2019)

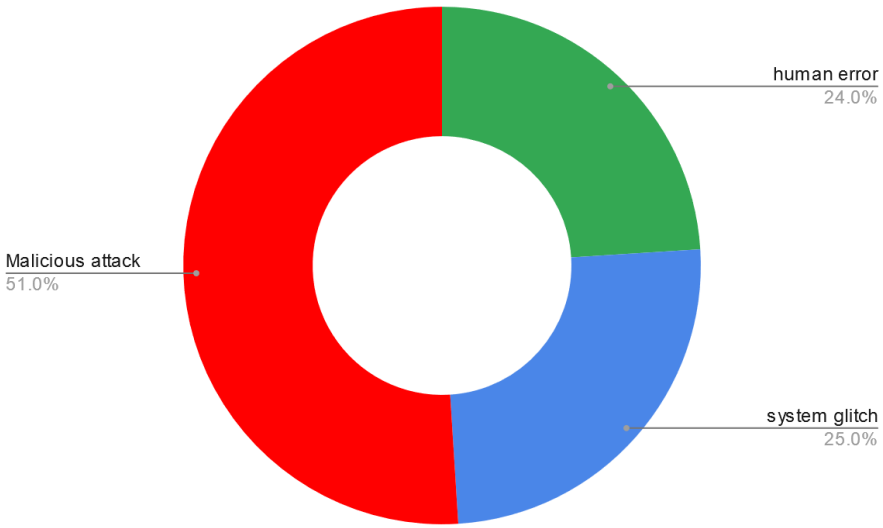


Figure 7 Causes of data breaches (adopted by Ponemon institute 2019)

This chart illustrates what are the causes of breaches, as well as how common they are. Unfortunately, 51% are malicious attacks on the company, followed by equal shares of system glitches and human error at 25% and 24%. Malicious attacks, since they most likely come from an outsider are not only the most common, but the costliest. In previous charts, it shows that the cost per compromised record could be $150 each. (Ponemon Institute, 2019) (IBM, 2020)

The prices for certain pieces of information vary, but social security numbers can be purchased for as low as $1. This is very surprising, since social security numbers, or SSNs are the key in a lot of finances. The price of your identity can rise if it can be associated with other pieces of information. For example: your name, birth date, SSN, and bank account numbers can be worth up to $30. The most expensive and desired records that are sold on the dark web are for US passports, going for about $1500. (Ellis,2019)

Another disturbing trend in the fraud market involves using children's SSN numbers. Otherwise known as creating a “synthetic identity”, an unused authentic SSN is attached to a false name, and then can be used to open various types of accounts, despite most of them having the age requirement of 18.

Children are the top targets due to them having a clean credit history, making it easy for “them” to get accepted for cards. Although originally SSNs were tied to birthdate, and region, in 2011 they were changed to be random. In doing this, it made it easier for hackers to steal identities, since they had no date or location limitations. In some cases, hackers have had luck in randomly guessing numbers, even ones that had not been assigned yet. This is also possible due to the extremely limited checks on numbers when signing up for various accounts, and kids are the ideal targets due to the unlikelihood of them checking their credit reports because they are underage. (O’Shea,2018)

The debt can accumulate over years, and most likely goes unnoticed until the kid becomes an adult and tries to apply for a credit card, only to be denied.

With various ways of hackers using information to open credit cards in different names, the industry estimated a total loss of $31.3 billion back in 2018, an 18% increase each year from 2013. With such a rich industry, it is no wonder why data is a popular item traded on the dark web. (Accenture consulting, 2017)

2.8 Malware

Malware, or also known as malicious software covers a wide variety of software used in order to cause destruction and hopefully gain information in the process. These programs can target computers, servers or a network. Malware consists of various programs such as: trojan horses, viruses, worms, trojans and many others. In summary, it can be bad when it ends up on your computer and compromises its and potentially others security.

Computer viruses usually fall into one of a few groups in their programmed behavior. The first computer virus, a worm virus called a creeper. Worms got their name from a 1975 novel by John Brunner, called The Shockwave rider. In this book, a data collecting worm is created to get revenge on an electronic information web that forces people to conform. (Brunner, 1975)

Creeper was written in 1971 by Bob Thomas who was working at BBN technologies, known as Bolt Beranek and Newman Incorporated. Although it was originally created as an experiment, that was rather harmless in nature, that changed when it was sent onwards to Ray Tomlinson. The harmless virus would hop between computers, deleting itself from the previous one and displayed a message that stated, “I am the creeper: catch me if you can”. However, Tomlinson, a colleague of Thomas, decided to modify the code to not delete previous copies of itself and to slow down the infected machines until they could no longer work. To combat the creeper worm, that was getting out of control, a reaper program was created. This is the first known anti-virus software to have been created. Fortunately, it did not do much damage, due to the limited amount of computers available. (Daakov, 2020), (Dominguez, 2019)

So, what makes the worm virus unique is the fact that it can self-replicate on its own, without a host. This feature makes worms probably one of the most troublesome viruses of all since it is easily transmitted.

The most famous worm attack occurred in 2008, going by the name of conflicker, a combination of the words: configure and flicker. This worm still exists today, although it is not as bad as it was at its peak. This worm was able to link Microsoft operated computers, creating a botnet of millions of computers. In other words, after connecting nearly all the world’s computers, approx. 15 million; an illegal super-computer was made.

The way the conflicker worked, was once it infiltrated the system; gave itself administrator rights, connected to one of 250 domains to remotely download files, searched the network for more pc's (to try to infect the entire network), creates a registry key so it can run in the background, then finally, proceeded to delete any system restore points. Another thing that made Conflicker so difficult to catch was the fact that it kept generating domain names. Once it connected to the new domain, it downloaded an update for itself. (Shin, 2010)

This virus even managed to penetrate national defense networks, such as the armed forces in Germany, UK ministry of defense, French navy and multiple hospital machines such as MRIs. In the code there was a countdown to April 1st, known as April fool's day, when the clock hit that day, it was supposed to scan for instructions and create a huge network, bringing most of the internet to a grinding halt.

Fortunately, when the day came, nothing happened. The virus was still there though, and needed to be stopped, so a group called the CWG, the Conflicker Working Group was formed, consisting of IT professionals from various fields. The idea of creating a group that could work together and create lines of communication between companies and governments to help find and hopefully prevent future large-scale cyber-attacks from happening in the first place. (Novan, 2018)

Lucki, with later updates to Windows operating systems came better security and seemed to leave the virus behind with Windows 7. The CWG group was successful in containing the spread of the virus by blocking domains that allowed it to update and spread, also what helped was the increased coordination internationally and creating procedures on how to deal with threats. The group expressed their perceived failure in that they could not help computers that had already been infected and could only slow down if not stop the spread to others. (Goodchild, 2011)

Eventually the worm was neutralized by blocking the worm from communicating with the one or ones who created it. The creator(s) of the worm were never found, nor did there appear to be a reason behind creating it, which is unusual.

The next type of virus is known as a Trojan virus. This type of virus got its name from the infamous Trojan horse used by the Greeks during the Trojan war to enter the city of

Troy, thus securing their victory in the war. The way this horse worked was that it was presented as a peace offering gift, but once it was wheeled inside the city's gates, the horse opened to reveal soldiers hidden inside of it.

Trojans are successful due to humanity's curiosity, by misleading its victims by hiding their true intent. This is the same as the Trojans and their gift, you too are also likely to click a link that says you have won something. Trojans can have several goals in their attacks, but most often they are for installing a backdoor on your computer, allowing the hacker to find out your personal private information and have control of your computer.

There are several types of trojans, such as backdoor, ransom, DDOS, and many more. Trojans are also able to attack mobile devices such as phones via hackers making fake apps on unofficial app stores. The user downloads a program, but unintentionally also downloads the trojan as well, which now has access to the information stored in the device. (Grace, 2020) (McAfee, 2020) Once the information is retrieved from the program, it can potentially be held for ransom.

Ransomware is a type of malware that can block you from accessing your files by encrypting them until a certain sum is paid. This can be accomplished various ways from clicking a link in an email to plugging in a mysterious usb port. There are two types of ransomware: crypto and locker ransomware. Crypto ransomware, the more common type of attack encrypts files, leaving the victim unable to access said files until a stated ransom is paid. Locker style attacks work in a similar way of locking the user out, but instead of it being files, they are completely locked out of the device itself.

Ransomware attacks can be targeted, such as one that occurred this year (2021) to the gaming company called Cd projekt red. The company was quick to tweet out a statement stating that an actor breached their network and encrypted some of their devices used in the company. After the encryption, a ransom note was sent out, which the company also released to the public.

The company made additional statements saying that despite this attack, that there were plenty of back-ups in place, and disconnected all compromised computers from their network. The company made a statement of refusal to pay any ransoms and did not care about hackers threatening to release confidential documents/data they claimed to have.

It is fortunate that the company was prepared in this situation, but they did have warning due to other gaming companies being attacked in the previous years.

Despite all these actions, however, the hacker group did get away with some stolen secret data and claims that they also obtained a copy of one of their unreleased games. According to Ke-la, a self-proclaimed "global leader of darknet intelligence", an auction for said data took place, with the bidding price starting at $1 million, or $7 million to buy. No one knows for sure how high the bidding went, and in addition, who bought it. Rumors point to cd buying it up to protect their intellectual property, or a competitor to gain insight into the company. (Abrams, 2021)

In contrast to an attack targeted at a specific company, some ransomware casts a wider net to catch as many people as possible. One notable example, called WannaCry in 2017 was devastating and managed to spread to over 150 countries. The estimated damage and financial losses caused by this attack was a worldwide $4 billion. WannaCry is defined as a "crypto worm", or "a form of malware that spreads in the form of a worm and encrypts victims' data" (Wiktionary, 2018) The way the worm worked was that it targeted Microsoft operating systems, and encrypted the data, then demanded a ransom be paid using bitcoin cryptocurrency.

Before the exploit was released, the group warned individuals of an impending attack, and Microsoft windows was able to release a security patch for it two months beforehand. Unfortunately, many computer users ignored the update or did not know how to download the update.

The ransom amounts varied between $300-600 and if it was not paid within three days, the user was notified that all their files were going to be deleted. It is always good advice to not pay ransoms, since there is no guarantee of the hacker holding up their end of the deal. Secondly, if the hacker knows that you will pay, it can make you a target again in the future. Since there was no way of identifying who paid and who didn't pay, the hackers wouldn't even know which systems to unlock. This crypto worm was said to have compromised over 230 000 computers and hit the NHS hospitals the hardest. As stated in the article: "ambulances were rerouted, leaving people in need of urgent care.

It was estimated to cost the NHS a whopping £92 million after 190 000 appointments were canceled due to the attack." (Kaspersky,2020) (Department of Health and Social care, 2018)

Backdoors are now easier and cheaper than ever to acquire. With as little as $5 for a tiny computer, called a raspberry pi zero loaded with malicious code called "poisontap" by Samy Kamkar, it can gain access within 30 seconds. This works by plugging it in via usb and tricking the computer into thinking that it has been plugged into the ethernet port, taking over the internet traffic for the entire system.

Odds are, that the user who logged out of their computer has the web open on it, so the device "continues to run HTTP requests in the background...intercepts all unencrypted web traffic and then sends the data to an attacker-controlled server." The inventor goes on to add that on some secure websites with an HTTPS domain are not set up correctly, data can be extracted from there too. (Storm, 2016)

Rootkits work in a similar way but are even more subtle. If a backdoor is a door, then a rootkit is comparable to a mousehole. A rootkit gets its name from "root", referring to root level access it gains from the system and "kit" referencing that it is software based, for implementing the attack. Rootkits are very difficult to detect, due to them masking themselves as part of the software that has administrator rights in the system. Rootkits also have been known to exploit vulnerabilities such as backdoors that may already be present in a system.

2.9 Phishing scams

Phishing scams are the most popular way for hackers to gain access to supposed secured internal systems. It got its name due to the similarity it has with fishing. The sea of fish are the users in this scenario and the lures are set out by hackers. The "ph" beginning most likely is since the earliest internet hackers were called phreaks. (History of phishing, 2019)

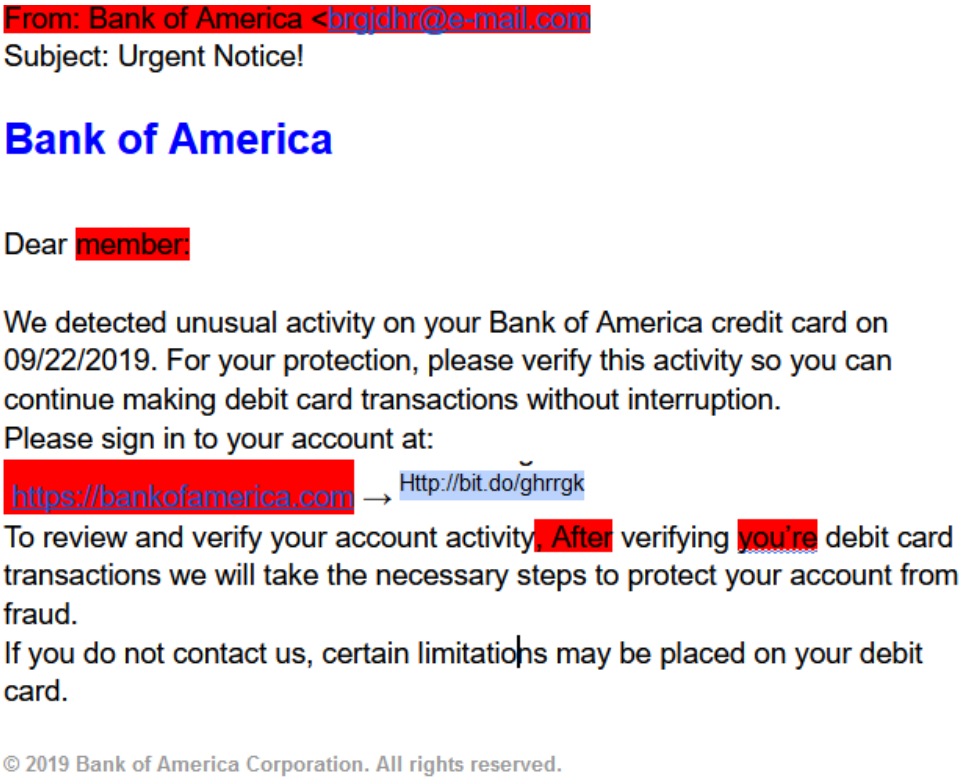
Phishing is interesting in how it works because it uses social engineering. A practice of using social interaction to gain the trust of the user. Humans tend to trust others and believe that they are naturally good, especially if the email seems harmless, or appearing

to come from a trustworthy organization. These emails often have a theme of an emergency, telling the victim to act fast or face unwanted consequences. The victim usually panics and clicks the infected link or sends over their information. Other emails seem too good to be true, such as the Nigerian prince scams, where a man wants to send you millions of dollars, but all he needs is your personal information.

Humans are emotional creatures, and emotions drive most of our actions, sometimes making us act on impulse instead of thinking things through. Therefore, the emails are structured the way they are, and why they are so effective. This works by having two different systems for thinking. The first system helps with immediate choices, whereas the other helps make slow and deliberate choices. Throughout the day, humans make thousands of decisions, many of which they are not completely aware of. Examples of these two systems are choosing where to sit versus what beverage to have. Phishing works, because it exploits the first immediate response which is what we use when feeling like there is a potentially urgent situation. (Schenkman,2020)

There are 3 main reasons why phishing is so effective:

1. Lack of computer knowledge and computer security. One example of this would failing to recognize if a website is legitimate or dangerous to go to, like ebay.com versus e-bay.com-security. Other things to look for such as the lock icon in the address bar to see if a site is secure or not.
2. Visual deception, seemingly legitimate text or confusing language being used. Links can appear to lead you somewhere, but when in fact, they go somewhere else entirely.
3. Lack of attention. This point refers to users failing to notice lack of security, or not noticing how when you hover over a false link it displays a different address. (Dhamija, 2006)


From: Bank of America <brgjdhr@e-mail.com
Subject: Urgent Notice!

Bank of America

Dear member:

We detected unusual activity on your Bank of America credit card on 09/22/2019. For your protection, please verify this activity so you can continue making debit card transactions without interruption.
Please sign in to your account at:
https://bankofamerica.com → Http://bit.do/ghrrgk
To review and verify your account activity. After verifying you're debit card transactions we will take the necessary steps to protect your account from fraud.
If you do not contact us, certain limitations may be placed on your debit card.

© 2019 Bank of America Corporation. All rights reserved.

Figure 8 phishing scams (adopted from onlineowls)

Above is an example of a phishing email, that has been circled in key areas. Upon a brief inspection of this email, which appears to come from a well-known and trusted bank that many people in the US use, it could cause the victim to panic. In the US banks typically send you emails and text notifications about card alerts, so this does not seem unusual to them. The sender appears to be from Bank of America but does not possess an official email address from them. This is the first red flag. Many scams come from outside native English-speaking countries, so there may be spelling errors or things are not capitalized when they should be. Lastly, the link that is given appears to go to their official website, when you hover over it displays the actual site it will direct you to.

The best way to see if this email is legitimate or not is to go to the actual website manually and login to check, or to call/visit your bank and see. Many companies also appreciate being informed of these scams to warn others who may not be as informed as others. Many companies make blanket statements, for example: if the company appears to have contacted you, they will never ask for your username and password.

Some companies have even managed to catch phishing scams due to them using a different terminology, like in the UK they say, “bank transfer” and scammers often use “wire transfer” and sign off using “cheers” instead of “thanks”. Luckily, this would be

easy to spot, even for those who may not know that these scams exist. (Gee, Swinhoe, 2019) There are quite a few varieties of phishing, all having the same end goal; to pose as a fake individual via email to gain access into secured systems.

One of the first types of phishing scams is called spear phishing. What makes this different from phishing is that spear phishing is more targeted at individual research projects at a given university. With the desire to share information to progress the research, many do not bother looking up who sent them the email to see if this is an actual legitimate person or a scammer.

Spear phishing has been traced back to about the year 2010 and has been more desirable since it has proven to be ten times more fruitful for getting sensitive information, since you are more likely to open an email that appears to be from a friendly source. (Brecht, 2015)

Spear phishing is a targeted attack, but has evolved into a new type of scam, called a "watering hole attack". How this works is that a hacker has an intended group or organization they want to infiltrate, but cannot do so directly, so instead a website or websites they frequent are infected. This style of attack got its name due to predators in the wild waiting at watering holes to attack animals when they least expect it. For example, an individual can be careful on strange websites, but a website they frequent and trust, they would let their guard down. In some cases, it could be a file that claims to be an update to your adobe player, something that many would not question in authenticity. (Paganini, 2012)

In 2013, the United States department of labor website's site exposure metrics tool was compromised. This tool was mainly used by workers and contractors to make or dispute a claim if someone was injured or exposed to harmful materials on site. The tool instead, redirected to a different page that had exploited and compromised the individual's computer. (Mimoso, 2013)

In addition to spear phishing, there is also the crime of whaling. This is where a high-level employee is targeted and manipulated into giving information or to pay a ransom. This can go both ways, a fraudulent email sent to a person that is high up in the company or appearing to originate from a person high up in the company.

The latter has a high level of success since employees often do not want to question or refuse an order from a superior in the company in fear of consequence, as mentioned earlier this is a process called social engineering. (Kaspersky, 2020)

Back in 2016, snapchat, a popular photo oriented social media platform suffered a whaling phishing attack. This resulted in an HR representative giving information on the pay of some of its past and current employees. The email was not even questioned as to if it was authentic or not, because it appeared to be from the head of the company. Luckily, the error was spotted within four hours, the FBI was contacted, and the affected employees were offered two years of insurance monitoring and identity theft protection. (Hern, 2016)

One of the last examples of phishing attacks would be called clone phishing. This is where a previous legitimate email with a link is sent, but then copied and edited. The link would redirect to a harmful page, most likely containing malware. There are luckily ways to spot a clone, you can check the email address that it is from. At first glance it will appear to be from a trusted sender, but upon closer inspection you will see it is from a stranger. Often hovering the mouse over a link will tell where it really directs to as well. Making a link appear to be to a certain page, when instead it is to a completely different page is called link manipulation. (Dutta, 2019)

The final example is most likely the oldest example of phishing. This is called baiting. Baiting is where a usb flash drive that is infected is left somewhere visible. This is like a real world trojan horse. The success of this type of attack depends on human curiosity, to take a flash drive or disc and put it on a computer to see what is on it. Sometimes for emphasis the item will have “urgent” or “confidential” on it to pique the individual’s curiosity even more. At the end of the day, it’s never a good idea to put anything into a computer that you do not know what is on it, especially on a secured computer. (Nadeem, 2020)

2.10 DDOS and botnets

Distributed denial of service, or DDOS attacks have been around since August 1999, but many do not know what came before it. DOS, or simply denial of service had been around since 1974, a whole 25 years before. Even though these two attacks have very similar

names, they are different in execution. DOS are much simpler to accomplish because they only need one computer and one internet connection to send a flood of requests to a certain server, with a goal to interrupt its connection between the hosting service of the site and the internet. The individual may have several reasons for wanting to do this, but it is usually because they do not want others to be able to access the site.

The first DOS attack was carried out by David Dennis, who was only 13 years old at the time. He managed to hack into the University of Illinois across the street from his high school via their shared computer education software, PLATO. He discovered that he could run a command for "ext." (external), allowing the computer to enable external devices. This froze the terminal up once the computer froze up when it realized that there were indeed no external devices attached. Instead of stopping there, having his curiosity satisfied, it led him to want to try to have this command be sent to multiple terminals at once, creating a mass lockout. He succeeded in this, and locked out all 31 users, but sadly for him, soon after this attack the command was then turned off and fixed the problem. (DDOS chronicles, 2017)

DDOS, a younger version of this attack is different in the way that it uses several different computers that have been infected by one main computer. One of the fastest growing in popularity and one of the most devastating types of attacks. These attacks are harmful because it can prevent legitimate users from accessing the network and can render it unusable. (Yihunie, 2018)

These infected computers are often referred to as zombies, or more commonly, bots. A network of all these devices is known as a botnet. The individual, or individuals who control the said zombie devices is known as a botmaster. How botnets are controlled depends on what type of architecture is used, but operate automatically versus manually, and can be IRC (Internet relay chat), HTTP (hypertext transfer protocol), DNS (Domain name system) or P2P (peer to peer) based. Next, there are usually one or more command and control servers, known as (C&C). C&C maintains the connection with the bots, in addition to managing them. Botnets are most used to carry out DDOS attacks but can also be used to send out spam emails with great efficiency. It is estimated that about 80% of spam emails are sent via botnets. (Hoque, 2015) (Nazario, 2008)

Botnets have 5 stages: initial infection, secondary injection, connection, malicious command and control, update/ maintenance. The initial infection is when a hacker scans systems for exploitable vulnerabilities and infects the system. Secondly, during the injection stage, the computer executes a fetch command via "shell code" to access a complete bot blueprint through http or ftp. After the injection phase, the bot is essentially ready to use. Next, the connection stage, where the bot connects to the controller to receive commands and can be controlled however the botmaster wishes. (Feily, 2009)

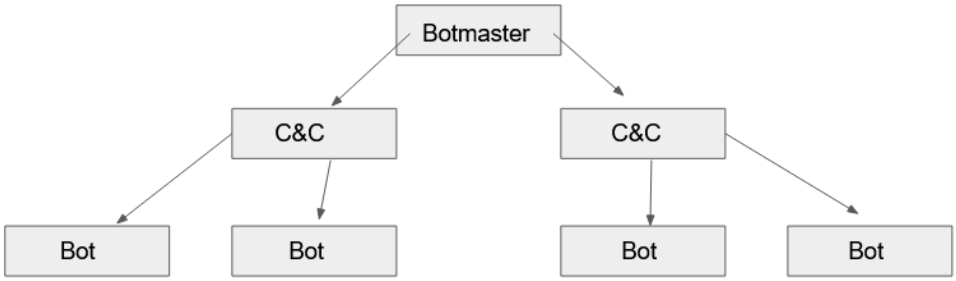


Figure 9 A Centralized botnet

Botnets can either be centralized or decentralized in nature. Centralized botnets use C&C servers to help manage the bots in the system and take orders from the botmaster themselves. An example of this would be in the form of a hierarchy.

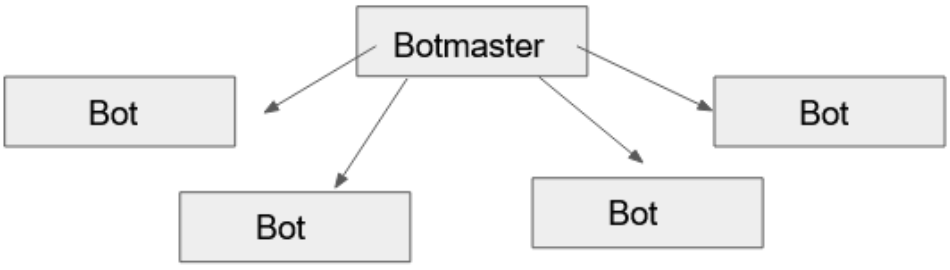


Figure 10 A Decentralized botnet

A decentralized botnet there are no specific C&C servers to help manage it. The bots themselves communicate peer to peer (P2P), keeping track of how many bots there are as

well as getting and giving information. An example of this would be the conflicker virus, as discussed in this study.

ENISA (European Union Agency for Network and Information Security) states that botnets are the most dangerous threats that face the world of cyber security today. Due to the increase in popularity of internet connected devices for convenience, this has led to the term being created: the internet of things. In the early days of internet connected devices, there were only computers, but now it expands to even refrigerators! (Bederna, 2020)
Common targets tend to be devices already in shared networks, such as university computers since they have a wide range of devices connected to it. Once the network is breached, the hacker can compromise all the systems, making it quite an efficient attack.

Computers can seem to work fine, but once the lead one sends a command through a shared server, it will be out of the owner's control. Botnets often vary in size, from a few up to hundreds of them all connected to each other. Due to the attack being connected to a net of computers, this makes it incredibly hard to trace, as well as very difficult to stop once it is started. The lead computer often has covered their IP address, making it appear to be in a totally different location than they are. Furthermore, in tracing difficulty, once the command has been sent to the bots, the attack starts, requiring a very limited connection.

The first use of a DDOS attack happened in 1999, at the University of Minnesota's 114 computers in their network got infected with a bad script called "Trin00". Trin00 caused the computers in the network to send so many requests that it made the entire school-wide network unusable for 2 days. The popularity of DDOS style attacks spread from there and quickly gained popularity when people realized how effective they were as a tool to take down a chunk of the internet. (ArXiv, 2019)

According to Trend micro's research paper, a DDOS attack to take down a small website can cost $30-70 for a day and goes up to a month for $1 200. (Goncharov, 2012). There are several types of DDOS attacks, the first one being called a buffer overflow attack. To understand what type of attack this is, first it must be broken down. A buffer is a term used for temporary storage set aside for a certain task. Most likely this storage checks to make sure the incoming data is correct to protect against attacks.

In any given system there are storage limits, now the overflow part of this attack comes into play. The input of data gets to a point where it exceeds the memory and can overwrite previous requests in the system. An example of this could be a login to a system with requirements between 6-12 characters, the system anticipates up to 12, but several requests of over 12 can potentially overload a poorly equipped server. (Imperva. 2020) C as well as C++, the most used programming languages unfortunately do not have any built-in protection due to their older age, whereas newer languages such as java and c# have some protection against it.

Within buffer overflow attacks, there are two main types of executions of it: a stack, or heap overflows. Stack attacks are easier to execute, therefore are more common. The stack, or the part of the memory used to store addresses as well as data, and once overloaded it crashes. The hacker then can reset the system and have it direct to a malicious site.

Secondly heap overflows, the hacker overflows the storage set aside for the program verses for storage. This, as you can guess, is harder to execute and is as a result, less commonly used (ukessays.com, 2018) (Cloud flare, 2021)

There are options on preventing these, such as monitoring the system and not allowing it to take on more requests than it can take on, otherwise called a boundary. Secondly, it can be programmed into a system, by telling it not to process anything over its limit.

The Ping of death, known as POD, or ICMP flood (internet control message protocol) abuses the ping command by overflowing the system with pings. The pings are also fragmented, making it difficult to piece together. The total size is also over the limit of 65 536 bytes which can destabilize the system or even crash it. (Candrlic, 2016) (Imperva, 2020)

Lastly, a SYN flood, where syn stands for synchronized consists of a system that does not complete all the actions necessary for the user to connect to the internet, and instead have the system overflow with internet connection requests, and therefore preventing anyone from connecting to the internet.

There are a handful of groups that use DDOS as a form of attack, such as the previously mentioned lizard squad. The Lizard squad never seemed to want a ransom, unlike other

groups who operate by sending emails to their future victims before the attack demanding to be paid (usually via bitcoin). These different groups focus their attacks on certain sectors and utilize different styles of attacks to exploit various vulnerabilities.

One example would be if the group called the Armada collective, a group that attacks the financial sector services hosted in Russia, Switzerland, Thailand and Greece. (Lobo, 2018)

2.11 Environmental and sociological risks

It is no surprise to anyone to learn that with increasing demand on technology, there has been a greater devastating impact on our environment. Although various types of technology have a seemingly never-ending list of benefits, and its enabling of connecting the people despite distance better than ever before, it also has a dark side.

With a seemingly insatiable demand for what is newer and faster, the market is finding it more and more difficult to keep up. In the year 2020 there are over 4.6 billion devices connected to the internet that previously had reached 1 billion users in the year 2000, a 360% growth in just 20 years. (internetlivestats, 2021)

With increased production comes a greater demand for power, and with limited renewable resources applied, fossil fuel is used. Combining fossil fuels and lack of proper disposal of hazardous materials in technology, pollution has gotten out of control. Microplastics have been found in humans, as well as animals and can be fatal to both.

“This trend has continued this year, with all five risks in the environmental category being ranked higher than average for both likelihood and impact over a 10-year horizon. This follows a year characterized by high-impact hurricanes, extreme temperatures and the first rise in CO2 emissions for four years. We have been pushing our planet to the brink and the damage is becoming increasingly clear. Biodiversity is being lost at mass-extinction rates, agricultural systems are under strain and pollution of the air and sea has become an increasingly pressing threat to human health.” (global risk report, 2018)

Ironically enough, contaminants can be damaging to datacenters, whether it be from pollution in the environment, or dust including fibers and filaments can do serious damage

in these centers. A way to avoid this is with filters and special suits that people wear when visiting them.

One of the major components when it comes to internet related technology is that it requires databases to work. These databases are located all over the world for ease of access. Several environmental factors can affect how well these data centers can perform. One of the most common occurrences is fire. Due to the high temperatures and often limited space, fires can spread through data centers quite rapidly. This can hopefully be avoided by implementing a fire suppression system that can quickly be deployed to limit the damage caused by the fire.

Lastly, power failure. Sometimes this can be unavoidable depending on the region. Power outages can be caused by a variety of situations such as an overload, or lightning storms. The best way to be prepared is by having back-up generators to limit or avoid down-time.

For a well-equipped data center, it is best to be prepared for anything and everything, with alarms and sensors to alert about changes in the environment from temperature, vibration or even humidity changes in the air. Constant monitoring of the environment will help preserve the center, and therefore the data it is hosting.

With the current situation in 2020-2021, the Coronavirus, servers are needed more than ever, with a wide amount of business and learning being now conducted via distance, aka online. Servers are, without a doubt feeling the strain of this drastic increase in traffic and usage of their systems, making it now more important than ever to keep everything up and running.

2.12 Risk response options

Whenever a disaster strikes, it is important to have the correct response. Having the wrong response can potentially make it worse and can damage the reputation of your company. In addition, the damage could potentially grow more severe, and, in this section, the different types of responses will be discussed for the individual to be empowered to pick their own appropriate reaction.

The first option is avoidance, which is defined by Richard Long as; "the elimination of hazards, activities, and exposures that can negatively affect an organization's assets." (Long, 2016). There is simply no risk involved in a certain activity if you do not partake in said activity in the first place. In other words, if a risk is simply ignored. This strategy works well and is the only 100% effective option in avoiding risk but can also negatively impact a company. Risk avoidance is seen as a negative reaction, versus a positive one since it promotes inaction instead of action. A company that takes no risks at all can do poorly in a competitive environment and potentially lose out to another one that is willing to take calculated risks. (Fennelly, 2017)

Following avoidance comes a similar response, risk reduction. Reduction works in the way that it acknowledges the risks involved in an action, but instead of inaction, steps are taken to hopefully reduce the damage or chances of it happening. Some examples of this include installing security cameras on the premises to deter or catch criminals, or for investments, to diversify them. This is achieved by quantifying potential liabilities and evaluating the risks they present. (Investopedia, 2019)

Sharing is the third choice on this list, it is also known as risk distribution. The name is easily misunderstood as making someone else bear the weight of the risk if it goes awry. This is fortunately far from what it is, and it refers to spreading out the risk to have the least damage possible if something does go wrong. There are multiple examples of this, and society uses this in most services for the public such as social security for retirement, insurances that clients pay for in case accidents happen and taxes for infrastructure, and government workers (i.e., police). (Phillips, 2017)

There are separate types of risk sharing, one of the most common is outsourcing. Outsourcing means when companies perform certain services outside of the business itself. This has many advantages, such as lower costs to the company and the company does not hold any responsibility for them. (Risk Sharing, 2018)

Some of the most outsourced activities are sales and marketing, IT related services, accounting, human resources, delivery, and logistics. Outsourcing is becoming increasingly more common, due to the low cost and especially if it is hard to find someone locally who specializes in the service that the company is looking for. The company itself

can then focus on something else, and not worry too much about the outsourced activities, since they delegated the responsibilities onto another company. (Dinu, 2015)

This is great for the company itself, but if not carefully managed, can lead to a lot of downsides. Communication can be difficult, especially if the company you outsourced a task to is far away, which can lead to interruptions in service or misunderstandings. Depending on how far apart the companies are, clashing cultures or language barriers could prove a challenge as well.

If outsourcing grows unmanaged for too long, it holds the potential of having the main company lose control of it. Quality standards might not be met, leading to disputes and maybe even in some extreme cases: legal trouble. Companies must also be careful to not outsource too many of their services due to the appeal of saving money, because they could lose the trust of the people who work for the company, and potentially customers.

Although outsourcing often comes with a lower price tag, one must weigh the pros against the cons before deciding, and the true cost for the company must also be weighed against it. (Kluyver, 2012)

The last option is retentive, or simply choosing to absorb and accept all the risks. This is the least favorable option, but also a valid choice when the company feels that they themselves can handle the responsibilities associated with it. For example, if getting insurance costs more than paying for the damage yourself, it may not be worth it to get the insurance in the first place. Risk avoidance and risk absorption often get mixed up. One way to keep these two terms separate, is if retention is absorbing all the risk, then avoidance would be to simply refuse to accept any of the risks. (Yakinyomi, 2020)

In order to run a successful company, risks must be identified and given a proper response plan. This will help the company to pre-determine the path they will take if x happens and how the plan from that varies if y happens. A healthy mix of all these responses is needed because different problems have varying levels of severity as well as damage associated with them.

2. 13 Literature review summary

Cyber risks are also a newer category when it comes to risk management. A cyber risk is the same thing as a cyber-threat, referring to any other type of attempt to breach a secure system. In other words, cyber risk is the first form of risk management to exist purely to mitigate risks in the digital world. (Britt, 2017)

With the growing popularity comes individuals that may form groups in order to disrupt services of the internet, and access information that is supposed to be confidential. These people are motivated by different reasons but present a problem for the information security. Hackers in the modern days have discovered that information can sell for more money and once into the system they are potentially able to access hundreds or thousands of people's personal details. In the United States, if someone discovers your social security number, they can potentially steal your identity and it can take years to get it back

Hackers are known for targeting several information rich industries, the top three would be the financial sector, health care sector/government and, with increasing popularity, schools. It is surprisingly that universities are a target, but this is most likely due to their rich personal information about students and staff that is not stored in secure ways. Even if you are not a student, and just merely applied to the school, your information could be at risk.

When data has been accessed without permission, it is called a data breach. What makes data breaches so dangerous is the fact that once the data has been leaked, it is almost impossible to remove it from the internet. It can spread quickly on hidden internet black-markets. The value of information varies, such as social security numbers for about $1. In contrast, the most expensive and most sought after are passports that go for about $1500. (Ellis, 2019)

Malware, malicious software is a hacker’s best friend, a tool for them to cause destruction and enables them to gain information in the process. Malware has been around since the 1975, when the first virus was created: the creeper worm. There are different types of malware, such as trojan horses, viruses, and worms.

A worm virus is unique because it can self-replicate, even without a host. It goes from computer to computer until a whole network is infected, making it hard to stop or remove. Secondly, a trojan horse virus. Trojans can hide their true harmful nature under a seemingly friendly exterior. One example would be a pop-up saying you won something, only to lead you to a site that installs a backdoor in your computer. A backdoor is one of the goals of a trojan horse, because it allows the hacker to gain access to the system later. Ransomware is one of the most popular trojan horses, it often encrypts your files until you pay the ransom, a certain amount of currency. Unfortunately, most ransoms do not end positively, and most pay without ever gaining access to their data.

Phishing scams, like the word fishing, work in similar ways. Hackers send out bait, usually in the form of an official sounding email that is urgent. What makes phishing scams interesting is that they are so effective due to social engineering. (Schenkman, 2020)

DDOS attacks, standing for distributed denial of service attacks utilize a network of computers to carry out an attack. A group of infected computers are referred to as zombies, or bots, and these bots form what is called a botnet. (Nazario, 2008] Botnets usually operate in five stages: initial infection, secondary injection, connection, malicious command and control, updates/maintenance.

With an increasing demand for newer, better technology, there is an increased strain on the environment. As of 2020 there are over 4.6 billion devices that are connected to the internet, and with an even greater amount of technology that is in the landfill. (internetlivestats, 2021) With all this waste, CO2 emissions are at an all-time high, leading to an increase in extreme temperatures, and more disastrous events such as hurricanes are being reported.

All the above are the various types of risks one must navigate when it comes to the internet, but luckily there are several ways on how to respond to them. Avoidance, most likely the least realistic one, requires the individual to not take part in any risky activities, and to play it safe. It promotes inaction versus acting. (Fennelly, 2017). Risk reduction is another type of response, in which the individual acknowledges the risk, but steps are hopefully taken to reduce the chances of it happening, or at least to contain the damage. This can be installing security cameras. (Investopedia, 2019)

Sharing is the third choice on this list, it is also known as risk distribution. The name is easily misunderstood as making someone else bear the weight of the risk if it goes awry. This is fortunately far from what it is, and it refers to spreading out the risk to have the least damage possible if something does go wrong. There are many examples of this, such as social security for retirement, taxes for infrastructure, and government workers (i.e., police). (Phillips, 2017) Outsourcing is a type of risk management, and refers to when companies perform certain services outside of the business itself. The one who is being outsourced to takes on the task(s) and takes on the risks. There are upsides such as having a specialist, and cheaper costs, but there are also downsides. There can be various problems, such as unclear communication, different customs and being far away from each other. Lastly, if it goes unmanaged, the company can lose control of them.

3 METHODOLOGY

There were various methods utilized in order to complete this thesis. Due to the different references and sources needed, both qualitative and quantitative data are used. For example, for the widespread interviews, qualitative data was collected and then made into pie charts to show the division of answers. This was primary data, collected by me, with the help of google forms. This survey saw thirty-five respondents, many of whom were online acquaintances and members in group chats I take part in. This was a simple solution to get a diverse sample size, and having it be easily completed in a few minutes online. The questions were multiple choice, offering a range of answers that they could pick from. The survey was open from November 10-15, 2020. Google forms helped record the data for me, making it easy to write about, and share the generated result charts.

For the individual interviews, qualitative methods were used. Instead of simple yes or no answers, more in-depth questions were asked, in order to get a better understanding of what the individual thought. These interviews were made possible by my thesis advisor Kirsi Aaltonen and featured four individuals. These interviews were structured, with pre-written questions to ask, but also offered space for the interviewee to ask or add anything they felt was important. The interviews were all held on the same day, November 11, 2020.

Getting both interviews and surveys completed was proven slightly difficult due to the current times of the Coronavirus and having to complete these studies at home from a distance, versus face to face. Luckily, however it seems more people are available and have free time due to this, so it has both positives and negatives.

Other data collection charts, displaying quantitative data, such as the ones present in the data breach section were gathered from existing data from third party sources. These were collected from different sites, and reports. The figures featured in the data breach and top targets section come from the Ponemon Institute, cost of a data breach report 2019. This was selected, due to its legitimate source and plentiful information it offered.
In this type of research, hindsight is always 20/20, but I do believe that the different combination of collection options was needed in order to analyze different data values. It is easiest to analyze numerical, quantitative data, but unfortunately it does not work for everything.

Therefore, I felt that the interviews were very important to gauge how people feel and respond to different situations, that may not always be able to be seen in a black and white way.

I approached this thesis using a qualitative method, in which I collected data from individuals, then proceeded to examine it and tried to spot certain patterns or similarities in it from the answers I received. This approach was taken due to not having previous hypotheses that needed disproving or improving.

The results of this study are that individuals in the 18-40 age group are more aware of safe internet practices than I initially thought they were. This is a relief, since this age group is most associated with being of the age to be in University, as a student, or as a newer staff member in the school.

Education on safe practices on the internet is important for anyone, especially what could be users that will have access to secure intranets with private information, in addition to education, re-education and updating said knowledge is equally important to maintain said security of information.

4 FINDINGS

4.1 University of Oulu ICT plan

There are some examples of plans put in place by universities, but unfortunately not all have a well thought out strategy put in place. This can mean disaster for the school if students and staff are not made aware of the potential risks and scams out there on the internet. The University of Oulu has a form that all students must read about their student accounts before they can use it. The form has 11 points on it, and it is short but gets to the point. This short list of guidelines makes it ideal for students, since they are more likely to read a piece of paper instead of a drawn-out booklet about the risks involved in having a student account linked to the university. It is important for all to read especially students, since they may come from different backgrounds and different ages with various levels of internet experience, making education about the potential dangers very important.

The guidelines go as follows:

1. You are responsible for all activities carried out on your user ID, never tell anyone your password. Remember to protect others information in addition to your own

2. Choose a password easy to remember but hard for others to guess

3. Don’t open email messages if you are not certain of their origin

4. Beware of phishing, messages asking to share your user ID and password or enter them on a website. System admins will never ask for your password

5. Always check the target address before clicking a link, some may be genuine while others could be fraudulent

6. Before registering as a user of an online service, check terms and conditions to make sure the data ownership will not be disclosed to third parties

7. Be careful of pop-ups and advertisements, click carefully

8. Use a firewall and antivirus on your own computer with back-ups. Also have a lock code on your phone and do not install unnecessary applications

9. Do not use only USB flash drives to store data, especially sensitive data

10. If you print out something on a shared printer, pick it up immediately

11. If you suspect a security breach or system abuse, contact person in charge of service immediately.

The University also has several guidelines for what makes a good password under ICT services. In order to even get your password accepted, it must be at least 12 characters long and can go up to 32 characters. Of these characters, there has to be both upper and lowercase letters, and numbers but not special Scandinavian letters used. Also, words found in the dictionary or number sequences and geographical locations are not recommended. Examples of good and bad passwords are given, to help the user create a strong login. (ICT services, 2019)

Students' data is being used by the University for various reasons but comply with Universities act legislation. Students are made aware that their information is being used to enable access to personal and contact information, process applicants to implement study rights, process exam enrollments, organize teaching in addition to exams, organize entrance and level exams, maintain study records, provide counselling, provide records of studies and diplomas, generating statistics and lastly protecting information security of students and staff. The information stored is name, security number, birth date, student number, username, background information, admissions information, nationality and language skills. They also share contact information for students. The reader is assured that the information is only handled by appointed personnel and in a secure way. All the places where the personal data is sent to is disclosed on a list of companies/organizations, providing transparency for the reader.

The student is also made aware that they are able to access this information and withdraw their consent, as well as updating incorrect information.

There is also a section on the website where you can email someone at the University if you are concerned about how your data is being used. (University of Oulu, 2020)

There is also a separate list of guidelines for mobile users intended for both staff and students. The list states that portable devices are a high risk since they can easily be misplaced or stolen. When this occurs, there is a risk of unauthorized access of your accounts and the thief posing as them online. In order to minimize the risk of not getting your phone back, the university recommends writing down your device's IMEI code and personalizing your phone to make it easily recognizable. Most phones also allow you to set a security pin code that isn't easily guessable (i.e., not a birthday or an easily guessable number series), also do not let others see your security code and change it if you think they have. Lending your phone to others is also potentially a big risk, especially if you are not present for when they are accessing it. You should always try to back up your data somewhere too, so you do not lose important stuff. This is important in case of the phone breaking, or theft. Finally, if you lose your device, it is important to try to erase its content remotely and notify the IT support about it, and when you are ready to discard the device, you should transfer all data and set it to factory settings. (Oulu University, 2020) There is a course on Moodle available, separate ones for students and teachers but is called "basics of information security for students/staff".

4.2 Analysis of ICT plan

The ICT plans that the University of Oulu has on its home site are very hard to locate and are not emphasized on the first pages for students. This is somewhat understandable due to the amount of information needed to be presented towards students, such as housing and tutoring. Where the information should be, it is not, such as the case for it being absent on IT services for students. There is a separate section intended for students, yet it doesn't appear to have any information on internet security guidelines. There is also no information under the new students' section, which could be very helpful.

The security information can be found at a separate section, at oulu.fi/ict. I personally found this undergoing to the contact section and then navigating to ICT services. This was not very intuitive for me. I spent several minutes looking through the section for students, and then after not being able to find any information relating to internet security for students, I decided to expand my search to the other pages. Another possible way to access these pages is to simply search for it, but that is not something that everyone would necessarily seek out information for.

For the most accurate information, I set out on completing interviews with four individual students at the University of Oulu. Due to the current pandemic, it was difficult to try to find more people, or to attempt these interviews in person. One upside to this, was completing these interviews online, and having the ability to save the actual interviews, making it easier to go back and reference them for the sake of documenting the answers accurately. These individuals are anonymous for the sake of the survey, so they can feel confident to answer freely and truthfully without any potential consequences.

Questions :

1. How often do you login to the school's internet services?
2. Have you read the internet security guidelines?
3. Would you click a link in an email if it was from a stranger?
4. Would you click it without question if it was someone familiar?
5. How many devices do you use?
6. Do you leave your accounts signed in on your devices?
7. Do you use any 2 step authenticators for security?
8. What, if any social media platforms do you use?
9. How often do you change your password?
10. Do you share accounts with other people for any service?

Figure 11 Survey questions

Here is a copy of the questions I asked the individuals for their interviews. Ten questions seemed to be a good amount, since it was not too few or too many. Interviews were conducted via teams and held over the course of a few days, due to both parties having busy schedules.

4.3 Individual interviews

Interviewee one

The first candidate said that they login to the school's internet services a few times a day at least because they have gotten into the habit of always checking it every weekday. When I asked if they had read the internet security guidelines, they said they had not read any, but they might have seen some at some point in time. The third question asked if they would click a link from an unknown sender, to which their answer was a firm no. This was good news, and led into the fourth question, which they said that they would not

click a suspicious looking link if it appeared to be from someone that they knew. The individual stated that they use two devices to use the internet: cell phone and a laptop. Despite not logging out of accounts, they close their laptop, and it logs them out, and it is password protected.

The individual uses two step authenticator software for the vpn and library services, as well as the online bank authenticator software, which is becoming more and more common. They also seemed relieved that two step authenticator software is becoming easier to use as well as more reliable. LinkedIn and WhatsApp are the only social media platforms they use, both for professional use. Due to the school requiring complex and hard to remember passwords, they, like most, only change their password when the school service prompts them to. Roughly, ever 6 months. The last question, regarding sharing accounts, stated that they only share accounts with family such as entertainment services i.e., Netflix and for newspapers that can allow several users per account.

Interviewee two

The second individual states that they login to the school services almost every day, or at least a few times a week. Logging in to the school has become part of their morning routine, even on weekends. For the second question, they stated that they did not read the guidelines, and was not even aware that such a document exists. They do however, read every email from the IT services. "When you login for the first time with your account, you have all sorts of documents that you need to read through, and it’s really overwhelming and hard to remember everything you’ve read”, they said, almost like an information overload it seems. Despite this, they have been using online services before and have general security knowledge.

They would not click a link from a sender, especially if there was no message or what it was related to, but it would be easier to click a link from someone familiar. Luckily, they are aware of the scams related to impersonating people online, so would consider it before clicking the link if it sounded like the person or not. One thing that we both agreed on with this group of questions was that Finland has been lucky in avoiding scams, since the Finnish language is so difficult to learn, so you can tell if a native speaker is typing it or not. If you type regularly in Finnish, an email in English or in broken Finnish might set

off red flags to you. The second candidate also uses a laptop and a phone, and sometimes their TV for internet services.

They do not leave their accounts signed into their devices, and always make a habit to log out of them. For two step authentication software, they want a simple solution for the school and only use the banking authenticator software.

Facebook, following twitter posts without an account, as well as LinkedIn and WhatsApp are the only social media platforms they use. They change their password whenever prompted to with the reminder messages from the school, every 6 months. It is one of those things that is easy to remember, and it's difficult to change a password since you have to remember a complex string of numbers and letters. For the last question, they do not share any accounts with anyone and only use their personal accounts.

Interviewee three

The individual states they login several times a day to the school's internet services since it has become a habit. For the second question, they stated that they have read the internet guidelines when they first started their studies and checked for them again before the interview. Most of the rules were common sense, and things that they had been doing already when using the internet.

The interviewee would not click a link from a stranger and is used to getting these types of spam emails, as well as not clicking a link from someone familiar unless they were expecting one. Luckily, the school email does not seem to have as much of these emails, perhaps it could be a stronger security filter or the longer, more complex email address. This unfortunately does not seem to be the case for Gmail and outlook, which get plenty of spam emails. When it comes to the number of devices, they state that they use four: a personal phone, work phone, work computer and personal computer to access the internet.

When it comes to if they leave accounts signed in, they stated that they do this, but have a password/pin protected device, so it is still secure. Unfortunately, the school does not offer much two-step authentication software, but they do use the banking software to login to various accounts that way.

When it comes to social media usage, they use; WhatsApp and LinkedIn, Instagram, Facebook, as well as YouTube, and snapchat. This makes candidate number three the person who uses the biggest variety of platforms. For changing their passwords, they do the required reset twice a year, but do not change other passwords as often as they know they should. For some services that they are not logging into every day, it is easy to forget their password and they need to reset it. This technically counts as changing a password, but only to regain access to the account. For the last question, they stated that they do share accounts for subscription based digital entertainment such as Netflix, Hbo and Ruutu.

Interviewee four

The last candidate I interviewed said that they login to the school's services every day for work purposes and use the library as well as Moodle services the most. Due to distance teaching being implemented for the school year, they also login to zoom about three times a week. For the second question, they answered that they had read the internet security guidelines, as well as the security policy and documents related to phishing sent out by the IT staff.

The individual stated that they would not click a link from a stranger due to being aware of threats when it comes to opening things. Fortunately, due to a good spam filter, it is easy to avoid this by not many getting through in the first place. When it comes to if they would click a link if it appeared to be from someone they knew, they said they would most likely click links if it appeared to be from someone they knew if it did not look suspicious. For example, if it were part of a reply chain you would click it vs a new email with no explanation.

When it comes to devices used to access the internet, they have; two computers, two phones (one of each being for work and the other being for personal use), and an iPad for personal use. Instead of logging out of various accounts, they shut down their computer which is password/pin code protected and does not share what they are in order to keep the accounts and devices secure. When it comes to personal devices, their family knows their passwords, since they are often shared but contain no sensitive information on them. This response helped me have an answer to the last question, if they share any accounts: which was no, not for anything.

Getting to the question regarding the use of two-step authentication they do not use it for work purposes, due to the school lacking an official one, but do use them for personal use. Two examples would be the banking software, and the app for email. Early two-step authenticators were painful to use and were not reliable. Additionally, sometimes the ones that use your phone are not convenient if you are not prepared and have it nearby.

For my last two questions, they answered that they change their password when it is required, every six months, but agree that they should change it more often. It can also be hard to remember passwords for 20 different accounts for example. Lastly, they use Pinterest, WhatsApp, LinkedIn and browse Instagram without an account.

4.4 Interview analysis

All these interviews gave me an insight as to how internet security is viewed by individuals who attend the University of Oulu.

For the first question, all of the interviewees stated that they usually login once a day, if not several times a day, or at minimum; a few times a week.

For the second question, on whether they read the internet security guidelines, the consensus was yes. One individual even added that there are documents in the school email that are supposed to be read before using it. Following this, I asked if they would click a link in an email if it was from a stranger, luckily the answer was a unanimous no. This was very good news, since phishing emails are becoming more and more commonplace, to gain access to its private data.

As an additional follow-up, would they click a link if it appeared to be from someone they knew? The majority answered no, with one answering yes. Another thing that was pointed out to me was the fact that the school email has a good spam filter, so not many get through that. For question 5, I asked how many internets connected devices they use. Due to all the respondents having work and personal devices, it ranged from 2-5 devices. All had a phone, and a laptop, but some had a work phone and a personal phone, same for laptops.

Question 6 was an important question to ask, whether they leave their accounts signed in or not. Luckily, the consensus was that if they did, their device itself was secured via password. Walking away from the computer, was generally logging out of the device, or closing it (which essentially serves the same purpose. This is great, in terms of security, so no one can hop on to an account that has been left logged into the school services.

Following this, the 7th question asked if they used any two-step authenticators for their accounts. All the individuals use the banking software that is available in Finland, in order to login to secure websites. One even reported to be using a VPN (virtual private network), for an additional layer of security. VPN's work by masking your real location, and making you appear to be in an entirely different location. Only one person reported to be using a two-step authenticator for their email.

When it comes to social media usage, LinkedIn was the most popular answer. Due to its professional nature, a networking site is not surprising in the fact that it is popular. Another popular social media platform, WhatsApp was also common. WhatsApp is a free messaging service, where you can make group chats and even call one another.

Question number 9 was an important question, it asked how often they change their passwords for their accounts. Their answers were not surprising to me, since it would have been my exact answer as well. Every 6 months the school requires a change of password, due to the previous one expiring. When it comes to other accounts that are more lenient when it comes to changing your passwords, people often slack off without reminders to change it, often keeping the same one for a year or longer. One reported that they do change their passwords, but usually when they have forgotten their password, needing to reset it.

The last question asked if they shared any accounts, I added this because most of my friends share their Netflix accounts with friends and family, so I wondered if it was as widespread as I thought. Fortunately, the general response was no, or only for sites that allow several users per account, in the form of profiles.

4.4 Widespread survey

Due to this thesis being completed in the time of a pandemic, I reached out to people online to help get more data for my surveys. I was fortunate to receive 35 responses to it. My respondents were equally split between male, and female at 48.6%, with 3.8 as non-binary.

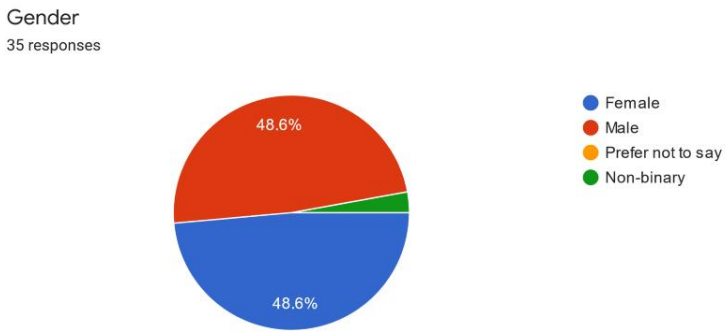


Figure 12 Gender

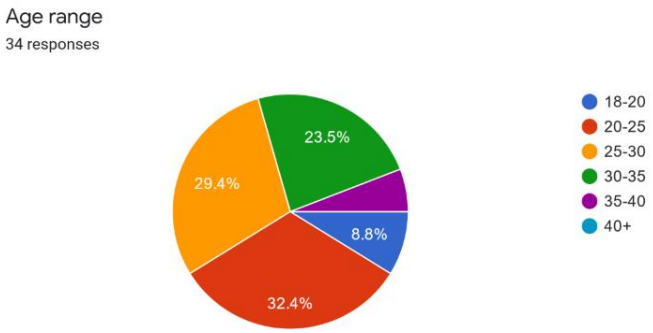


Figure 13 Age range

The age range on the results varies but has the biggest group of 20-25 at 32.4%. The second biggest group falls in the age range of 25-30 (29.4%), followed by 30-35 (23.5%). The final groups were 18-20 at 8.8% and 5.9% who were 35-40. Lastly, 51.4% of this group were not studying, leaving a 48.6% group that is currently studying.

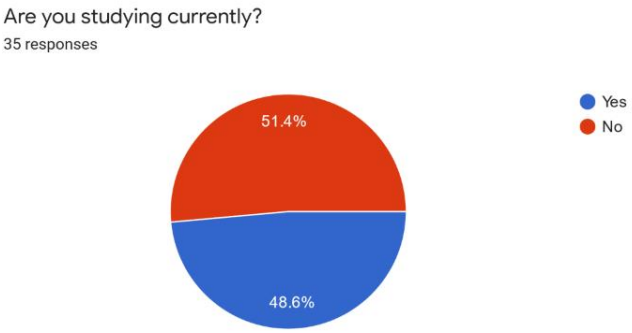


Figure 14 Occupation

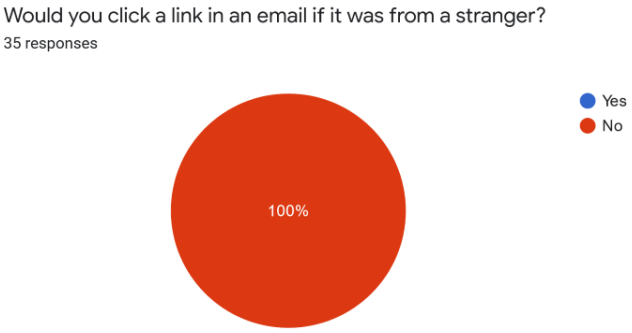


Figure 15 Clicking a link from a stranger

In contrast, if the email appeared to be from someone they knew, 68.6% said they would click it and 31.4% said they would not. This question was included due to certain viruses spoofing a real email from a trusted sender, when in fact it contains malware.

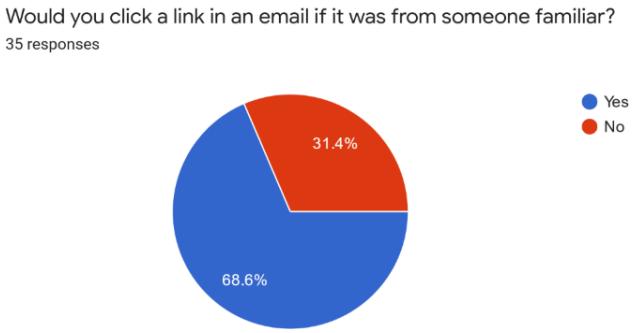


Figure 16 Clicking a link from an acquaintance

For the next question, I was curious to see how many devices they use to access the internet. The majority, or 60% claimed 3-4 devices, followed by a tie of 20% of 1-2 devices and 5 or more. This does not surprise me, because in 2020 there are an estimated 31 billion devices, and every second sees 127 new IOT (internet of things, is the name given to this expanding area of devices accessing the internet). By 2025 there are an estimated 75 billion devices on the IOT. This network not only includes phones, but the increased application of "smart" devices such as kitchen appliances. (Maayan, 2020)

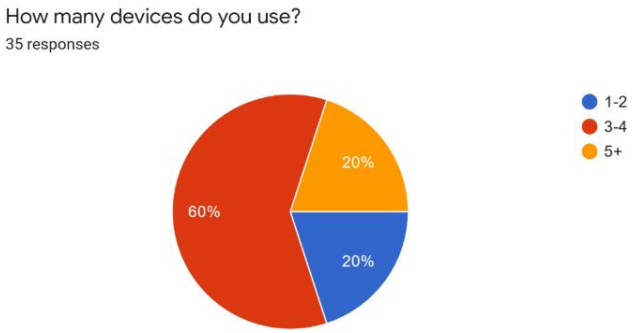


Figure 17 Device usage

Following this question, I then asked if they left their accounts logged into their devices. Majority, so 68.6% said yes, 22.9% said sometimes, for some accounts but not all, and lastly, 8.6% said no. With services being more convenient and keeping you logged in, sometimes it can be a hassle to login every time to use it. For example, the school's intranet logs out inactive users, but Netflix on a smart tv keeps you logged in until you click logout or change your password.

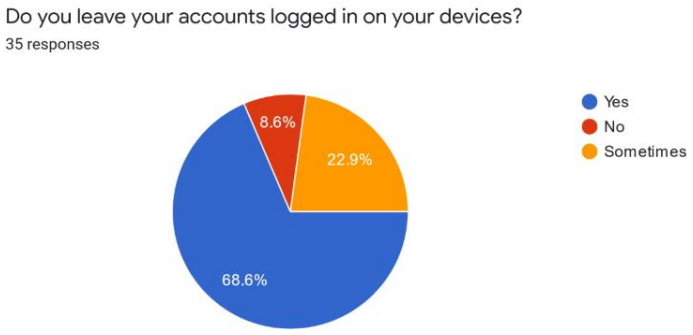


Figure 18 Accounts left logged-in

After this, I asked if they use any two-step authentication software, and fortunately 77.1% said yes, that they do use it. 22.9% said they do not, but it was not clarified if they do not use them because they did not know about them, or that they choose not to. There are ones that are part of the service, with email, or third-party ones. I think the popularity also had to do with the use of the online banking software that is widely used to confirm the user's identity.

Figure 19 Two-step authentication

I included a social media usage question because some of these platforms have been involved in controversy with their selling of user’s data for tailored ads targeted at them.

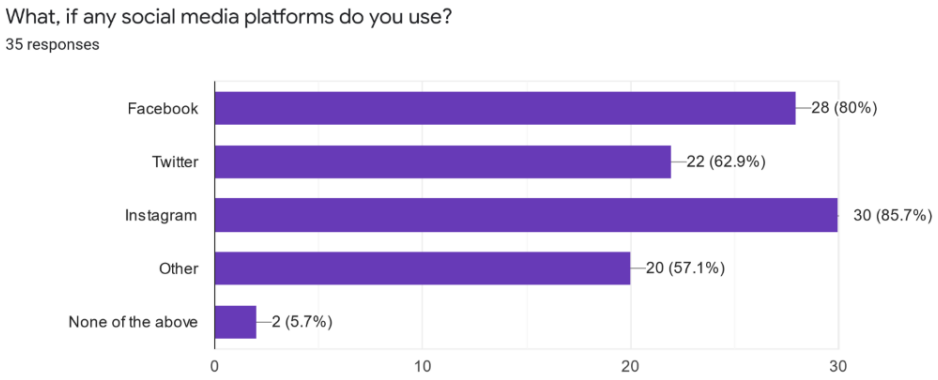


Figure 20 Social media usage

The most used platform was Instagram, with 85% of the votes. Instagram mainly focuses on picture-based posts and uses hashtags, or the pound sign # to better organize photos, but that is up to the user.

Facebook, the oldest social media on this list is second with 80% of the votes. This could be people keeping in touch with friends and family, as well as those who use their messenger messaging service.

Twitter, a text based social media that has a 240-character limit for posts, is next with 62.9% of the responses. Many individuals who have twitters do not post, or tweet themselves, but use the platform to follow celebrities and enter giveaways. This platform also utilizes the hashtag system.

There are so many social media platforms out there, it is impossible to write them all down. For the sake of sanity, I only included the top three biggest platforms that I know of. In the survey there was a big, 57.1% category of other, that makes me want to go back and add more platforms to make it less vague.

Lastly, adding none as an option, because there are people who like to completely avoid social media, for many reasons (ex: privacy concerns and the proven connection of it having a negative effect on your emotional well-being), but this category was only 5.7% of the respondents.

For the next question, I was curious to see how often individuals change their passwords. Different places have different recommendations, but it usually falls between six months to every year. It's understandable that people are averse to changing their password, especially if they've never had any experience with their accounts being compromised. Also, it is a pain to always be trying to remember your new passwords when you reset it.

In this question, the biggest category, by far, was they do not remember how long ago it was that they changed their passwords. This group consisted of 62.9% of the group. I find this shocking, but I too would fall into this category for most of my accounts.

Every year was next, at 14.3%, which was a large difference from the most popular. I am glad, however, that this is the second most popular response.

Every few months, followed at 11.4%, which is also great, I was surprised that there were such diligent people out there, and lastly every half year at 8.6%, and 2.8% claim they change their passwords every month. This question did not specify the accounts they change the passwords if, but I could see it varying per account.

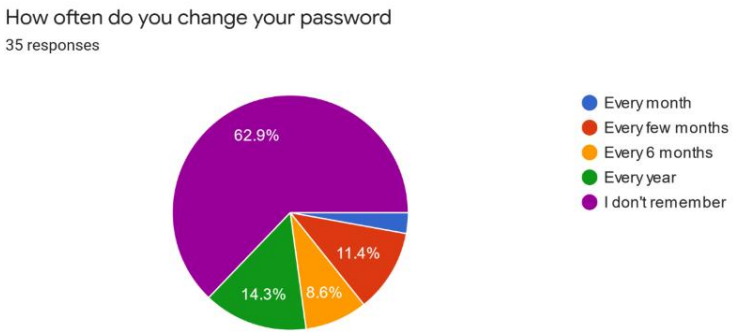


Figure 21 Frequency of password changing

For the last question: do you share any accounts with anyone? I wanted to include this because many people share accounts for subscription-based services, since they can easily add up in price if you own them all. If people do not share with friends, they probably share with family. But I got the exact opposite results from what I expected. Majority, 54.3% do not share their accounts with anyone. This is great for security and shows that they are responsible with their various accounts. Those who do share accounts were at 47.5%, which is still a significant amount, but still less than I was expecting.

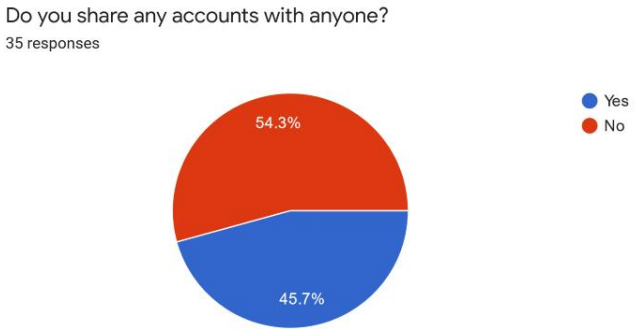


Figure 22 Account sharing

4.5 IT staff interview

After reviewing the University of Oulu's current ICT policy, it was time to interview the actual staff who are responsible for keeping the school's network secure. This is a crucial part of the thesis, since it is best to get information from the source. Thanks to a helpful member of the IT support, I was able to get answers to my questions.

My questions were, as follows:

1. Have there been any attacks?
2. If there was an attack what were they targeting?
3. Is there training for teachers to learn the risks of sharing information online?
4. About how many estimated active users are there?
5. Do you have a plan in case of a cyber attack?

Figure 23 ICT questions

For my first question, I asked if the university has a plan in case, it is ever targeted in an attack. Fortunately, the answer was yes, and stated that they annually take part in an exercise that practices the organization's ability to respond to different types of cyber-attacks. The program is called TAISTO, and its exercises in data protection and security breach management.

The second question asks if there have ever been any attacks? For security reasons, this answer had to be given in general terms, but there are several types of cyber-attacks that happen in the university. Phishing emails are quite common, minor data breaches, active ransomware attacks and staff members being targeted via phone calls using a spoofed, (or fake number that appears to be coming from a known source) that appear to be from fake technical support.

In order to get an idea of the internet traffic the university experiences on a daily, or weekly basis, I asked for the number of active users in the network. Unfortunately, this number is not exact, but currently there are about 3500 employees, and 25 000 students, making the number of active users several thousand.

Lastly, I asked if teachers receive any training on cyber security. The answer to this was also yes, and the training covers both data security and data privacy. The training material is made by an external vendor and university.

All in all, I was pleased to know that the university is prepared when it comes to a cyber-attack, and that the staff have been trained on cyber security in addition to data privacy. Also, participating in an annual exercise is also a great idea to test the response and effectiveness of what is already in place. The exercise also offers feedback in possible areas of improvement, without the danger of a real attack where the institution could lose confidential data.

5 DISCUSSION

There are many purposes of this research study, but most importantly it will hopefully serve as a good source of information for companies and universities on cyber security planning and risk management.

In addition to my offering a source of background information, it could also serve as a warning that universities are a newer target for cyber criminals due to them being unprepared when it comes to good security.

This study also shows examples of when organizations made the rest that choice or made the wrong choice and had to face the consequences of their actions. Hopefully this will educate more on the issue and shed light on how there's always a right way and a wrong way of doing things. Lastly, I want this study to improve various organization's approaches to educating students and staff on how to keep their accounts and information secure, in a world where cyber-attacks are growing more and more common.

The results were pleasantly surprising to me, I was happy to find out that most people have in the 18-30 age group the ability to stay secure online and know what phishing emails and scams are. I was worried that a user base as big as the university could potentially be a huge risk area, since there are thousands of active accounts that login daily.

The findings of this study are reliable, especially when it comes to in person and individual interviews. When it comes to the widespread survey, the findings may be less reliable since it was sent out and filled in by people who may or may not be telling the truth. However, since it was anonymous, people have very little reason to not tell the truth.

The research for this study is also reliable, due to many sources coming from books, or published journals, and the online sources were cross-checked with multiple sources to ensure that accurate information is used in this study. Websites that looked out of date, or were not run by an official news organization, or published by a known journalist were not used.

When writing this study, I learned a lot more about cyber-crime than I thought I would. The first documented crime was earlier in history than I thought it would be, and it would have taken place after the invention and wide adoption of the internet. This attack happening as far back as 1834 in France via individuals gaining access to a secure telegraph system and getting away with it because it was not technically illegal, seems so farfetched to me. (Standage, 2013)

I had basic information on this topic, but also learned more how different types of attacks work, such as botnets that are centralized or decentralized, or the fact that you can buy different types of DDOS attacks on the dark web.

Data breaches have been becoming increasingly common, since the first one in the 1980's took place with TRW. This was one of the most devastating breaches of what was supposed to be secure information for about 90 million people. (Diamond, 1984)

It is unfortunate that these breaches were not officially recorded until 2005, which makes information on them slightly harder to acquire and can potentially be unreliable if not cross-checked with multiple sources. (Privacy rights clearinghouse, 2020)

I was also surprised to find out that a lot of people do not continually change their passwords, since it is an easy thing to forget to do. The university requiring password resets every half year is a good idea, because that was the only password individuals seemed to continually change. Despite infrequently changed passwords, the staff and the students I interviewed were extremely knowledgeable about the topic of internet security, which was a relief to hear.

It was exciting to conduct interviews and find more out about the University of Oulu's plans they have in case of a disaster. Sadly, it could not be explained in detail due to the staff member signing an NDA agreement.

With this research, I hope to inform universities about the various types of cyber attacks there are out there, and just how harmful they could be if they were a victim of one. A data breach could leak confidential research and lose the school money. A phishing scam could cause student's and staff's information to be leaked, and a DDOS attack could crash the whole network and make the intranet services unusable.

With proper protection, however, these could all be avoided, or at least minimize the damage.

5.1 Future of risk management

Unfortunately, no one can accurately predict what exactly the future will hold, for pretty much anyone or anything. People can only predict and anticipate for the future, with their knowledge of the past and by charting how different areas are progressing to see where they are heading.

This thesis has proven that cyber-attacks are on the rise, and many industries are not fully prepared for it. With a world increasingly moving towards a more digital form, it will be interesting to see how different industries deal with it. The industry will grow, and the importance of it will become more apparent.

Kids are getting introduced to technology at young ages, by using computers for educational purposes, thus also becoming better equipped with knowledge on how to use various forms of computers. Most children, or teens are more knowledgeable than their parents, and grandparents, due to not growing up with it.

With an increase of technology-based intelligence, one would hope that cybersecurity would also be taught, and the importance of it stressed, to prevent disasters from occurring.

AI, or artificial intelligence is just at its beginning stages currently. Several assistants, such as Google, Siri and Alexa are thought to be AI, are just programmed to search for information and are incapable of truly "learning" much if anything. Other "AI " can also be effective at spotting patterns and anomalies in data, making it possible to be implemented in many industries, such as cyber security in the future. (Eling, 2018)

Deepfakes are also gaining popularity, in addition to AI learning. Although AI learning can be a good thing, it has the potential to be weaponized and could even automate cyberattacks. A deepfake is a combination of the words deep learning and fakes. Using catalogs filled with dozens of photos of a said celebrity, they can be scanned to create a realistic 3-D image that can be manipulated. The deepfake can even utilize audio clips and can be made to say anything. Various examples are out there, and some may seem harmless, like a lip-syncing celebrity up to a politician saying something they never would say. However, harmless or not, using someone's likeness without their permission is illegal, and in the future there will most likely be legal issues surrounding this, and doubts as to what is real and what is fake. (Kietzman, 2020)

Even though not everything about the future is certain, there are always going to be hackers, and there are always going to be cybersecurity to prevent hackers and breaches from occurring. The tools used by both sides will change and become more sophisticated over time, as shown in the background of hacktivism, but never has changed as a concept.

6CONCLUSIONS

This study will hopefully be educational and informative to those who choose to read it. In today's world with everything moving towards an increased amount of internet connected devices and a shift towards digital workspaces and shop fronts, it has never been more important to read up on cyber security, and the risks involved with going online.

The background on the internet, and the rise of activists shows how technology has been rapidly improving and that humans will always stand up for what they believe in, in the form of protest or informing the public of what is going on behind the scenes.

Different forms of data breaches inform the reader of just how many types of attacks there are, in addition to how they are carried out. Offering some examples of these attacks hopefully demonstrates just how dangerous they can be if unprepared.

The most frequently attacked, targeted industries serve to surprise the reader, because it is most likely not what they think they would be. Explaining why and how they have been attacked proves why criminals have had so much success when targeting these specific sectors.

One portion of this study was set aside for focusing a study on the University of Oulu, and how prepared it would be when it came to cyber-attacks. Students were interviewed to see how responsible and knowledgeable they are on the subject. Unfortunately, due to in-person interviews not being possible, a widespread survey of people within my age group was sent out and results analyzed from it.

Being informed of all the risks that are involved in decisions and security, it is important to make the right choices in order to keep information secure and away from those who attempt to steal it and sell it online, and everyone who reads this will be able to implement a successful risk management plan.

6.1 Managerial implications

There are many things to consider in order to implement an effective risk management strategy when it comes to online safety and security. Confidential information is the new gold for hackers, which is why it needs to be secured.

The first step for implementing a risk management plan is to identify any possible areas that may need improvement. This can take the form of users with weak passwords, up to an uneducated staff. While doing this, it is also important to take note of what you have, how desirable the information or data is, in order to get a general idea of how much protection you need.

After this, you can plan for an attack. There are various companies out there that work in security that will help you run simulations of how an attack would be carried out, without the downside of compromising your secure data. The company will help identify weak areas you may have, as well as areas of improvement. Like the University of Oulu, who does annual exercises in this to keep it up to date, regular drills are important to implement.

It is good to have security that is constantly being monitored, without any down or off time. It should easily be accessible in real time.

Lastly, develop plans on educating staff and students about cybersecurity, and make it the norm. Demystify it and offer information to every new user in the system, and a refresher courses for staff members to keep it up to date in their minds about how security is evolving. With all these steps, security is possible even with thousands of users accessing the secured network daily.

6.2 Recommendations for future research

Due to the constantly evolving form of the internet, it is without a doubt, always going to be an interesting phenomenon to observe. No one knows what will be different in the future, or what will be the same.

My recommendations for future research would be to observe how risk management strategies have changed over time. It would be interesting to observe if cybercrimes have increased, decreased or stayed the same. With the dark web, it is easy to buy several types of ready to go attacks, such as a DDOS for under $100. This, in other words, means that cyber-attacks are not limited to groups of people with certain skill sets, and are more accessible.

Are universities, the health sector and financial sector still the top targets? How has their security evolved to protect themselves, as well as regulations for their needed security systems?

Looking into if laws have come into place regarding punishment for hacking into secure systems and tracking down members of hacker groups.

In the future there could be other hacker collectives, both white and black hat hackers. It would also be an interesting idea to see what they will accomplish with their abilities.

I am also interested to see if Solid is successful, the form of decentralized internet that has been slowly gaining more and more traction. Solid has the potential to change the internet as we know it but could also potentially be snuffed out by the bigger corporations involved in running the internet.

REFERENCES

Accenture consulting, 2017 Driving the future of payments [online document] US, Accenture, 16p
[Accessed 1 March 2021]

Abrams, Lawrence, CD Prokekt's stolen source code allegedly sold by ransomware gang, [online document] Bleeping computer, 2021
Available from: https://www.bleepingcomputer.com/news/security/cd-projekts-stolen-source-code-allegedly-sold-by-ransomware-gang/ [Accessed 5 March 2021]

Andrews, Evan, 2019, Who invented the internet? [online document] History
Available from: https://www.history.com/news/who-invented-the-internet [Accessed Feb 15 2021]

Argaez, de Enrique, 2005 Internet growth 2000-2005, [online document] Internet world stats
Available from: https://www.internetworldstats.com/pr/edi008.htm [Accessed Feb 15 2021]

ArXiv, 2019 The first DDOS attack was 20 years ago, [online document]Technology review
Available from: https://www.technologyreview.com/2019/04/18/103186/the-first-ddos-attack-was-20-years-ago-this-is-what-weve-learned-since/ [Accessed: April 2020]

BBC Teach, 2016, The people are revolting- the history of protest, [online document] BBC
Available from: https://www.bbc.co.uk/teach/the-people-are-revolting-the-history-of-protest/zdpdgwx [Accessed March 7 2021]

Bamford, Scott, 2019, Reputational damage: 3 worst cases & 11 next steps for protecting your brand & company. [online document], Miratech holdings Inc
Available from: https://www.jdsupra.com/legalnews/reputational-damage-3-worst-cases-11-90321/ [Accessed December 15 2020]

Baraniuk, Chris, 2013, Whatever happened to the phone phreaks? [online document] The Atlantic

Available from: https://www.theatlantic.com/technology/archive/2013/02/whatever-happened-to-the-phone-phreaks/273332/ [Accessed April 20 2020]

Beattie, Andrew, 2020, History of insurance [online document] Investopedia
Available from: https://www.investopedia.com/articles/08/history-of-insurance.asp [Accessed April 15 2020]

Bernard, Tara Siegel, 2017, Equifax says cyberattack may have affected 143 million in the US, [online document] NY Times
Available from: https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html [Accessed March 23 2020]

Brecht. Daniel, 2015, A brief history of spear phishing, [online document] Infosec
Available from: https://resources.infosecinstitute.com/topic/a-brief-history-of-spear-phishing/ [Accessed March 23 2020]

Britt, Phil, 2017,Cybersecurity risk management: finding and fixing your security vulnerabilities. [online document] Esecurity planet
Available from: https://www.esecurityplanet.com/networks/cybersecurity-risk-management-finding-and-fixing-your-security-vulnerabilities/ [Accessed March 17 2021]

Bederna, Z, Szadeczky, T, 2020, "Cyber Espionage Through Botnets." Security Journal, 33.1 p. 43-62

Brooker, Katrina, 2018, Tim Berners-Lee, the man who created the world wide web, has some regrets [online document]Vanity fair
Available from: https://www.vanityfair.com/news/2018/07/the-man-who-created-the-world-wide-web-has-some-regrets [Accessed Feb 1 2021]

Brunner, J, 1975. *The Shockwave Rider*. New York: Ballantine Books (288) ISBN: 0-06-010559-3

Candrlic, Goran, 2016, Types of DDOS attacks, [online document] Global dots
Available from: https://www.globaldots.com/blog/types-ddos-attacks [Accessed May 15 2020]

CFI, 2015 regulatory risk [online document]
Available from:

https://corporatefinanceinstitute.com/resources/knowledge/finance/regulatory-risk/ [Accessed May 16 2020]

CFI, 2021, What is market risk? [online document]
Available from; https://corporatefinanceinstitute.com/resources/knowledge/trading-investing/market-risk/ [Accessed May 16 2020]

Christensson, Per, 2006, "Cybercrime Definition." [online document] *Tech Terms*
Available: https://techterms.com/definition/cybercrime [Accessed March 1 2020]

Clement, J, 2020, Worldwide digital population as of Jan 2020, [online document]
Statistica
Available: https://www.statista.com/statistics/617136/digital-population-worldwide/ [Accessed May 1 2020]

Cloud flare, 2021, What is buffer overflow, [online document]
Available: https://www.cloudflare.com/en-ca/learning/security/threats/buffer-overflow/ [accessed March 10 2020]

CMOC, 2017,. 6 ways to help identify a malicious emai [online document]
Computermediconcall
Available: https://www.computermediconcall.com/6-ways-help-identify-malicious-email/ [Accessed: March 1 2020]

CNB University, 2020,How banks limit risk in commercial lending [online document]
Canandaigua National bank and trust
Available:
https://www.cnbank.com/Your_Bank/Education_and_Advice/CNBU_Articles/How_Banks_Limit_Risk_in_Commercial_Lending/ [Accessed March 5 2021]

Coble, Sarah, 2020, Judge signs off on $7.75m Equifax settlement [online document]
Info security magazine
Available: https://www.infosecurity-magazine.com/news/judge-signs-off-775m-equifax/ [Accessed May 1 2020]

Cognos, 2020, Top 10 answers from the world's first Chief Risk Officer. Lam, James, Cognos IBM 02/08 P. 1-4

Crouhy M,. Gdai, D, Mark, R, 2006, Essentials of risk management. New York. McGraw Hill (672) ISBN: 0071818510

Daakov, George. Dominguez A, 2019, History of computer viruses: creeper and reaper [online document] Pandora FMS
Available: https://pandorafms.com/blog/creeper-and-reaper/ [Accessed: Feb 20 2021]

DDOS chronicles, 2017, History of DDOS attacks [online document] radware
Available: https://www.radware.com/security/ddos-knowledge-center/ddos-chronicles/ddos-attacks-history/ [Accessed December 3 2020]

Delio, Michelle, 2001, The greatest hacks of all time [online document] Wired
Available https://www.wired.com/2001/02/the-greatest-hacks-of-all-time/ [Accessed December 3 2020]

Department of Health and Social care, 2018, Securing cyber resilience in health and care [online document] UK, Cyber security policy 21p
[Accessed May 5 2020]

Denning, Dorothy, 2015,The rise of hacktivism [online document]
Available: https://www.georgetownjournalofinternationalaffairs.org/online-edition/the-rise-of-hacktivism [Accessed December 3 2020]

Dhamija, R., Tygar, J.D. and Hearst, M., 2006, April. Why phishing works. [online document]
In Proceedings of the SIGCHI conference on Human Factors in computing systems (pp. 581-590)
[Accessed April 25 2021]

Diamond, Stuart, 1984, Credit file password is stolen, [online document] New York times
Available https://www.nytimes.com/1984/06/22/business/credit-file-password-is-stolen.html [Accessed November 2020]

Dione, George, 2013, Risk management: history, definition and critique, [online document] Canada, Cirrelt 22p
[Accessed March 5 2020]

Dinu, A.M., 2015. The risks and benefits of outsourcing. [online document] Knowledge Horizons. Economics, 7(2), 103p
[Accessed April 25 2021]

Donovan, J., 2016. ‘Can you hear me now?' Phreaking the party line from operators to occupy [online document] Information, Communication & Society, 19(5), pp.601-617 [Accessed April 25 2021]

Dutta, Pallavi, 2019, A guide to “what is clone phishing?” [online document] Krakital blog
Available: https://www.kratikal.com/blog/a-guide-to-what-is-clone-phishing/ [Accessed May 1 2020]

Eiten, Kimberly, 2019, Baltimore ransomware attack| city inches closer to normal operation [online document] CBS Baltimore
Availablehttps://baltimore.cbslocal.com/2019/06/12/baltimore-ransomware-attack-inches-closer-to-normal/ [Accessed November 12 2020]

Eling, M., 2018. Cyber risk and cyber risk insurance: Status quo and future research [online document]
[Accessed April 25 2021]

Ellis, Will, 2021, How much does your data cost on the dark web? [online document] Privacy Australia
Available https://privacyaustralia.net/dark-web-personal-data/ [Accessed March 1 2021]

Emma, Mary, 2020, Story of Johnathan James who hacked NASA and pentagon in age of 15 [online document] Techasli Horoscope
Available https://techasli.com/story-jonathan-james-hacked-nasa-pentagon-age-15/
[Accessed May 15 2020]

Feily, M A. Shahrestani and S. Ramadass, 2009 "A Survey of Botnet and Botnet Detection," [online document] Third International Conference on Emerging Security Information, Systems and Technologies, 2009, pp. 268-273
[Accessed April 25 2021]

Fennelly, L, Perry, M, 2017, Part 2 - Assessing Risk and Vulnerabilities, Physical Security: 150 Things You Should Know. New York, Butterworth-heinemann, (185) Pages 79-96 ISBN: 978-0-12-809487-7

Finkle, Jim, 2015, Database of 191 million U.S. voters exposed on internet: researcher [online document] Reuters
Available https://www.reuters.com/article/us-usa-voters-breach-idUSKBN0UB1E020151229 [Accessed March 1 2021]

Fung, Brian. Peterson, Andrea, 2014,Meet the grinch who stole Christmas for gamers: the lizard squad [online document] Washington Post
Available https://www.washingtonpost.com/news/the-switch/wp/2014/12/26/meet-lizard-squad-the-group-claiming-responsibility-for-ruining-christmas-for-gamers/ [Accessed December 3 2020]

Goering, Z, C., and L. Thomas, P. (eds) (2018). Critical Media Literacy and Fake News in Post-Truth America, Leiden, The Netherlands: Brill | Sense. Available From: Brill https://doi.org/10.1163/9789004365360 [Accessed 27 March 2021]

Goodchild, Joan, 2011 [online document] Conflicker working group says worm is stopped but not gone. CSO
Available https://www.csoonline.com/article/2126743/conficker-working-group-says-worm-is-stopped--but-not-gone.html [Accessed March 15 2021]

Goode, L, 2015, Anonymous and the Political Ethos of Hacktivism, [online document] Popular Communication, 13:1, 74-86, DOI: 10.1080/15405702.2014.978000 [Accessed April 18 2021]

Goode, L, 2015, Anonymous and the Political Ethos of Hacktivism, [online document] Popular Communication, 13:1, 74-86, DOI: 10.1080/15405702.2014.978000 [Accessed April 20 2021]

Goncharov, Max, 2012, Russian underground 101 [online document] Trend micro research, US, trend micro 29p
[Accessed May 1 2020]

Grace, Alison, 2020, What is a trojan? Is it a virus or is it malware. [online document] Norton
Available https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html [Accessed May 1 2020]

Greenspan, Jesse, 2012, Jesse. Guy Fawkes day: a brief history [online document] History
Available https://www.history.com/news/guy-fawkes-day-a-brief-history [Accessed May 1 2020]

Hern, Alex, 2016, Snapchat leaks employee data CEO scam, [online document] The Guardian
Available https://www.theguardian.com/technology/2016/feb/29/snapchat-leaks-employee-data-ceo-scam-email [Accessed November 20 2020]

Hoque, Nazrul, Dhruba K. Bhattacharyya, and Jugal K. Kalita. "Botnet in DDoS Attacks: Trends and Challenges." *IEEE Communications Surveys and Tutorials* 17.4 (2015): 2242-2270

IBM, X-force threat intelligence index 2020, 2020 [Online document] IBM, US, 60p [Accessed March 20 2020]

ICT services, 2019, What is a good password? [online document] University of Oulu
Available https://www.oulu.fi/ict/node/11216 [Accessed March 27 2020]

Imperva, 2020, Buffer overflow attack [online document]
Available https://www.imperva.com/learn/application-security/buffer-overflow/
[Accessed December 3 2020]

Imperva, 2020, Ping flood (ICMP flood) [online document]
Available https://www.imperva.com/learn/ddos/ping-icmp-flood/ [Accessed May 23 2020]

Infosec, 2011, A history of anonymous [online document] Infosec resources
Available https://resources.infosecinstitute.com/topic/a-history-of-anonymous/
[Accessed June 12 2020]

Internetlivestats, 2021, [online document] World wide web consortium (W3C)
Available: https://www.internetlivestats.com/
[Accessed: May 1 2020]

Investopedia, 2019,Risk avoidance vs risk reduction [online document] Investopedia
Available https://www.investopedia.com/ask/answers/040315/what-difference-between-risk-avoidance-and-risk-reduction.asp [Accessed May 1 2020]

Kalat, David, 2018, The history of passwords and the case of the first theft[online document]Think set mag
Available https://thinksetmag.com/issue-6/the-case-of-the-purloined-password [Accessed March 20 2021]

Kaspersky 2020, What is a whaling attack [online document]
Available https://www.kaspersky.com/resource-center/definitions/what-is-a-whaling-attack [Accessed March 1 2021]

Kaspersky, 2020, What is WannaCry ransomware [online document]
Available https://www.kaspersky.com/resource-center/threats/ransomware-examples [Accessed March 2 2021]

Kietzmann, J., Lee, L.W., McCarthy, I.P. and Kietzmann, T.C., 2020. Deepfakes: Trick or treat?. [online document] Business Horizons, 63(2), pp.135-146.
[Accessed April 15 2021]

Kluyver, Cornelis, 2012, Fundamentals of Global Strategy. 8.4 risks associated with outsourcing, University of Oregon, (257)Saylor Foundation
Pages 169-194 ISBN: 9781453332870

Llewellyn, Gavin, 2019,Bond capital's annual 2019 internet report [online document] Smart insights 333p [Accessed May 1 2020]

Long, Richard, 2016, Defining risk avoidance for a modern business structure [online document] Mha consulting
Available https://www.mha-it.com/2016/11/30/defining-risk-avoidance/ (Accessed June 2020]

Lovelace jr., Berkeley, Gurdus, Lizzy, 2018,Hospital CEO forced to pay hackers in bitcoin teaches others how to prepare for the worst [online document] CNBC
Available https://www.cnbc.com/2018/04/06/hosptial-ceo-forced-to-pay-hackers-in-bitcoin-now-teaches-others.html [Accessed November 1 2020]

Lobo, Savia, 2018,The 10 most common types of DOS attacks you need to know [online document] Packtpub
Available https://hub.packtpub.com/10-types-dos-attacks-you-need-to-know/ [Accessed March 15 2021]

Lukasik, S., 2010. Why the ARPANET was built. [online document] IEEE Annals of the History of Computing, 33(3), pp.4-21
[Accessed April 28 2021]

Maayan, Gilad, David, 2020, The IOT rundown for 2020: stats, risks and solutions [online document] Security today
Available https://securitytoday.com/articles/2020/01/13/the-iot-rundown-for-2020.aspx [Accessed December 3 2020]

McAfee, 2020, Understanding trojan viruses and how to get rid of them [online document] McAfee
Available https://www.mcafee.com/blogs/consumer/understanding-trojan-viruses-and-how-to-get-rid-of-them/ [Accessed March 1 2020]

McCormick, Ty, 2013, Hacktivism: a short story [online document] Foreign policy
Available https://www.firstlinepractitioners.com/hacktivism/ [Accessed December 3 2020]

McKenzie, Lindsay, 2019,Cyberattacks mar start of academic year [online document]Inside higher ed.
Available https://www.insidehighered.com/news/2019/08/27/two-universities-targeted-hackers-just-new-school-year [Accessed March 27 2021]

McPherson, S.S., 2009. Tim Berners-Lee: Inventor of the World Wide Web.[online document] Twenty-First Century Books
[Accessed April 28, 2021]

Middleton, B., 2017. A history of cyber security attacks: 1980 to present. [online document] CRC Press

[Accessed April 15 2021]

Mimoso, Michael, 2013, Watering hole attack claims US department of labor website. [online document] Threatpost
Available https://threatpost.com/watering-hole-attack-claims-us-department-of-labor-website/100081/ [Accessed May 15 2020]

Miniwatts marketing group, 2019, Internet world stats [online document]
Available: https://www.internetworldstats.com/top20.htm
[Accessed April 15 2020]

Mohebzada, J. G, et al.. Phishing in a University Community: Two Large Scale Phishing Experiments. 2012, International Conference on Innovations in Information Technology (IIT) (2012): 249-254.

Morgan, Steve, 2019, Humans on the internet will triple from 2015 to 2022 and hit 6 billion [online document] Cybercrime magazine
Available https://cybersecurityventures.com/how-many-internet-users-will-the-world-have-in-2022-and-in-2030/ [Accessed March 20 2020]

Nadeem, M. Salaman, 2020,. Social engineering: what is baiting? [online document] Mailfence Updated
Available https://blog.mailfence.com/what-is-baiting-in-social-engineering/ [Accessed March 202020]

Nazario, J., 2008. DDoS attack evolution. [online document] Network Security, 2008(7), pp.7-10
[Accessed April 27 2021]

Novak, Matt, 2015, Nikola Tesla's incredible predictions for our connected world, [online document]Gizmodo
Available https://paleofuture.gizmodo.com/nikola-teslas-incredible-predictions-for-our-connected-1661107313 [Accessed November 1 2020]

Novan, 2018,Conflicker and its legacy: An overview of the conflickerworm [online document] Medium
Available https://medium.com/@donovan.adams/what-is-this-confiker-y-you-speak-of-an-overview-of-the-conficker-worm-eb4997928107 [Accessed March 10 2021]

Nycyk, M., 2020. From Data Serfdom to Data Ownership: An Alternative Futures View of Personal Data as Property Rights. [online document] Journal of Futures Studies, 24(4), pp.25-34
[Accessed April 28 2021]

Oreilly,2020,Classic problems of probability [online document]

Available:https://www.oreilly.com/library/view/classic-problems-of/9781118314333/chapter03.html

[Accessed March 20 2021]

O'Shea, Bev, 2018, How thieves are creating false identities using your child's social security number. [online document] The Denver channel
Available https://www.thedenverchannel.com/financial-fitness/how-thieves-are-creating-false-identities-using-your-childs-social-security-number [Accessed May 20 2020]

Oulu University, 2020, Mobile security guidelines for staff members and students, Oulun Yliopisto 2p [Accessed May 15 2020]

Paganini, Pierluigi, 2012,Phishing: a very dangerous cyber threat [online document] Infosec
Available https://resources.infosecinstitute.com/topic/phishing-dangerous-cyber-threat/ [Accessed March 20 2020]

Phillips, William, 2017,Insurance and risk sharing [online document] Phillips financial strategies
Available https://www.phillipsfinancialstrategies.com/blog/insurance-and-risk-sharing [Accessed Feb 13 2021]

Phishing org, 2019,History of phishing [online document]
Available https://www.phishing.org/history-of-phishing [Accessed November 20 2020

Pomeranz, J (1984) The Dice Problem—Then and Now. *The Two-Year College Mathematics Journal* 15:3, pages 229-237.

Ponemon Institute, 2019, Cost of a data breach report [online document] IBM, US, 35p [Accessed March 20 2020]

Poulson, Kevin, 2008, One hacker's audacious plan to rule the black market in credit cards [online document] Wired
Available https://www.wired.com/2008/12/ff-max-butler/ [Accessed May 1 2020]

Poulson, Kevin, 2011,The card master: why max butler crowned himself king of a global online fraud network [online document] Wired
Available https://www.wired.co.uk/article/the-card-master [Accessed May 1 2020]

Poulson, Kevin, 2001, Whitehat hacker made FBI patsy, [online document] The register

Available https://www.theregister.com/2001/05/09/whitehat_hacker_made_fbi_patsy/ [Accessed March 20 2021]

Privacy rights clearinghouse, 2020, Data breaches,[online document] Available https://privacyrights.org/data-breaches [Accessed March 1 2021]

Refsdal, A, 2015, Cyber-Risk Management. [online document] 1st ed. Springer International Publishing, 2015 (145) ISBN: 978-3-319-23570-7 [Accessed May 20 2020]

Rhodes, Angus, 2015, A brief summary of the long history of risk management [online document] Ventiv Available https://blog.ventivtech.com/blog/a-brief-summary-of-the-long-history-of-risk-management [Accessed May 1 2020]

Sambra, A.V., Mansour, E., Hawke, S., Zereba, M., Greco, N., Ghanem, A., Zagidulin, D., Aboulnaga, A. and Berners-Lee, T., 2016. Solid: A platform for decentralized social applications based on linked data. [online document] MIT CSAIL & Qatar Computing Research Institute, Tech. Rep [Accessed March 26 2021]

Schenkman, Lauren, 2020,Why we fall for phishing emails-and how we can protect ourselves, [online document] Ted Available https://ideas.ted.com/why-we-fall-for-phishing-emails-and-how-we-can-protect-ourselves/ [Accessed March 15 2021]

Segal, Troy, 2020, Operational risk [online document] Investopedia Available https://www.investopedia.com/terms/o/operational_risk.asp [Accessed May 15 2020]

Sharpe, James, 2018, Who was Guy Fawkes, the man behind the mask [online document] National geographic Available https://www.nationalgeographic.co.uk/2018/11/who-was-guy-fawkes-man-behind-mask [Accessed March 15 2021]

Shedden, David, 2014, Today in media history: The Internet began with a crash on October 29, 1969, [online document] Poynter Available https://www.poynter.org/reporting-editing/2014/today-in-media-history-the-internet-began-with-a-crash-on-october-29-1969/ [Accessed March 1 2021]

Shin, S. and Gu, G., 2010, December. Conficker and beyond: a large-scale empirical study. [online document] In Proceedings of the 26th Annual Computer Security Applications Conference pp. 151-160
[Accessed March 27 2021]

Standage, Tom, 2019, The first cyber attack happened back in 1834. This is the story [online document] Wonderful enginering.
Available https://wonderfulengineering.com/the-first-cyber-attack-happened-back-in-1834-this-is-the-story/ [Accessed May 15 2020]

Storm, Darlene, 2016, Hacker can backdoor your computer and router in 30 seconds with $5 poisontap device [online document] Computerworld
Available https://www.computerworld.com/article/3142131/hacker-can-backdoor-your-computer-and-router-in-30-seconds-with-5-poisontap-device.html [Accessed March 1 2021]

Stout, David, 2000, Youth sentenced in government hacking case [online document] NY times
Available https://www.nytimes.com/2000/09/23/us/youth-sentenced-in-government-hacking-case.html [Accessed May 1 2020]

Study, 2018, Risk Sharing: Definition, Strategies & Examples [online document] study.com
Available https://study.com/academy/lesson/risk-sharing-definition-strategies-examples.html [Accessed December 15 2020]

Stuster, Dana, J, 2013, Saudi Arabia bans Guy Fawkes masks for ‘instilling culture of violence’ [online document] Foreign policy
Available https://foreignpolicy.com/2013/05/30/saudi-arabia-bans-guy-fawkes-masks-for-instilling-culture-of-violence/ [Accessed December 3 2020]

Tariq, N., 2018. Impact of cyberattacks on financial institutions. [online document] Journal of Internet Banking and Commerce, 23(2), pp.1-11
[Accessed April 25 2021]

Tassi, Paul, 2015,Lizard squad hacker who shut down PSN, Xbox live and an airplane will face no jail time [online document] Forbes
Available https://www.forbes.com/sites/insertcoin/2015/07/09/lizard-squad-hacker-

who-shut-down-psn-xbox-live-and-an-airplane-will-face-no-jail-time/?sh=107d76782ecd [Accessed May 15 2020]

Tesla, Nikola, 1920, [online document] Colliers magizine
Available https://paleofuture.gizmodo.com/nikola-teslas-incredible-predictions-for-our-connected-1661107313 [Accessed November 1 2020]

Toma, Juliette, 2018, The couch jump that rocked Hollywood, [online document]The Ringer
Available https://www.theringer.com/tv/2018/8/1/17631658/tom-cruise-oprah-couch-jump [Accessed March 15 2020]

Traynor, Ian, 2007, Russia accused of unleashing cyberwar to disable Estonia. [online document] The guardian
Available: https://www.theguardian.com/world/2007/may/17/topstories3.russia
[Accessed May 1 2020]

Trend Micro, 2017, Flying under the radar: how hackers use protection strategies for attack [online document]
Available: https://blog.trendmicro.com/flying-under-the-radar-how-hackers-use-protection-strategies-for-attack/ [Accessed May 1 2020]

UKEssays, 2018. Buffer Overflow Attacks And Types Computer Science Essay,[online document]
Available from: https://www.ukessays.com/essays/computer-science/buffer-overflow-attacks-and-types-computer-science-essay.php?vref=1 [Accessed 5 March 2021].

University of Oulu, 2020, Processing student's personal data and the University of Oulu [online document]
Available: https://www.oulu.fi/forstudents/data-privacy-notice [Accessed May 15 2020]

Vincent, Jame, 2015,. Popular chrome extension Hola sold users' bandwidth for botnets. [online document] Business insider
Available: https://www.theverge.com/2015/5/29/8685251/hola-vpn-botnet-selling-users-bandwidth [Accessed May 1st 2020]

Wang, P. and Johnson, C., 2018. CYBERSECURITY INCIDENT HANDLING: A CASE STUDY OF THE EQUIFAX DATA BREACH.[online document] Issues in Information Systems, 19(3), pp.150-159
[Accessed April 25 2021]

Web foundation, 2012,History of the web [online document] world wide web foundation
Available: https://webfoundation.org/about/vision/history-of-the-web/ [Accessed May 15 2020]

Wellington, K., 2013. Cyberattacks on medical devices and hospital networks: legal gaps and regulatory solutions.[online document] Santa Clara High Tech. LJ, 30, p.139 [Accessed April 15 2021]

Wiktionary, 2018, Cryptoworm [online document]
Available: https://en.wiktionary.org/wiki/cryptoworm [Accessed March 1 2020]

Wills, Matthew, 2017, WWII and the first ethical hacker [online document] Jstor daily
Available: https://daily.jstor.org/wwii-and-the-first-ethical-hacker/ [Accessed May 1 2020]

Wright, A., Aaron, S. & Bates, D.W. The Big Phish: Cyberattacks Against U.S. Healthcare Systems. [online document] J GEN INTERN MED 31, 1115–1118 (2016). https://doi.org/10.1007/s11606-016-3741-z
[Accessed April 15 2021]

Yakinyomi, Timothy, 2020, Risk retention vs risk avoidance [online document] Medium
Available: https://medium.com/@timothyakinyomi/risk-retention-vs-risk-avoidance-9690437eed54 [Accessed May 5 2020]

Yihunie, F., Abdelfattah, E. and Odeh, A., 2018, May. Analysis of ping of death DoS and DDoS attacks. [online document] In 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT) (pp. 1-4). IEEE.
[Accessed April 25 2021]

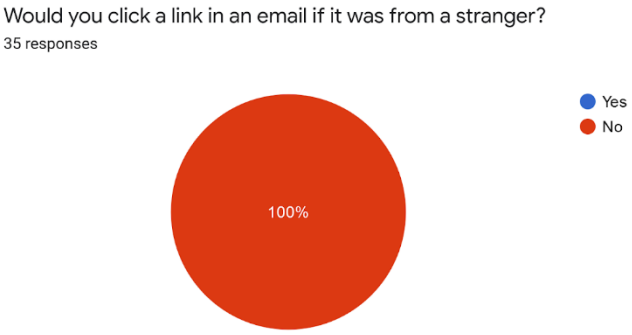
Yle, 2020, Psychotherapy center's database hacked, patient info held ransom [Online document] Yle uutiset
Available:
https://yle.fi/uutiset/osasto/news/psychotherapy_centres_database_hacked_patient_info_held_ransom/11605460 [Accessed October 21 2020]

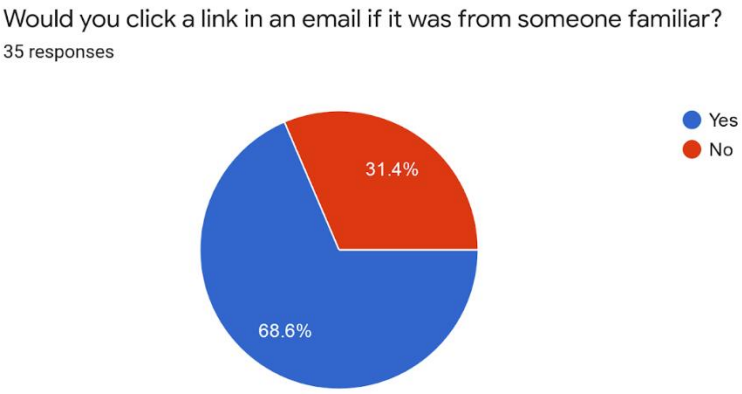
Youtube, 2011, Tom Cruise on Oprah [online video] [Acessed March 1 2021]

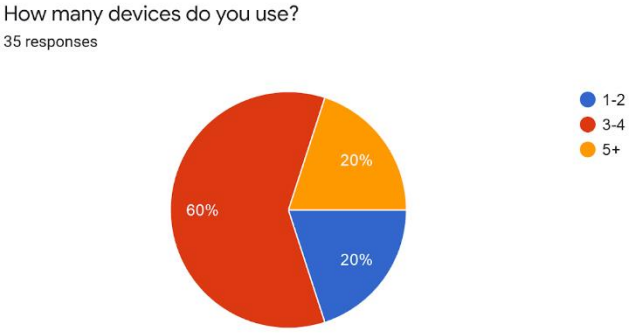
Zhenfang, Zhu. "Study on Computer Trojan Horse Virus and Its Prevention.", 2015 [online document] International Journal of Engineering and Applied Sciences, vol. 2, no. 8
[Accessed April 28 2021]

APPENDIX

Widespread survey questions and answers:

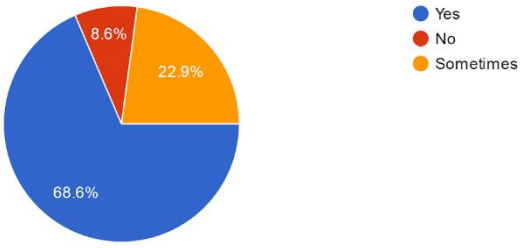






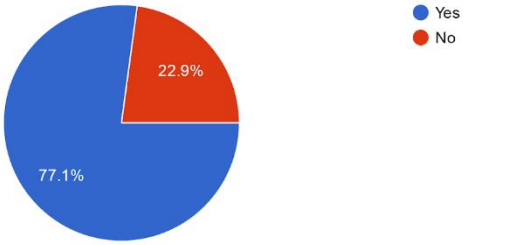
Do you leave your accounts logged in on your devices?

35 responses



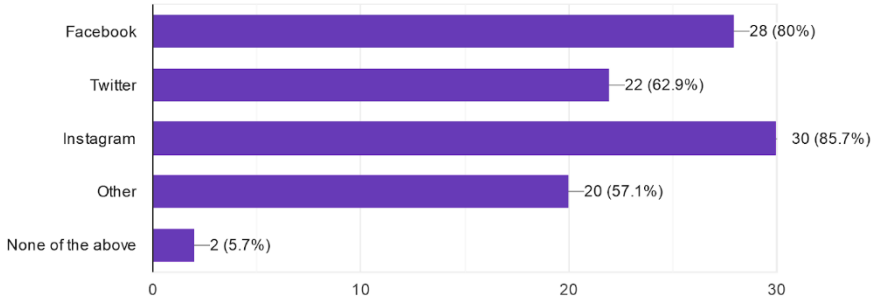
Do you use two-step authentication for your accounts?

35 responses



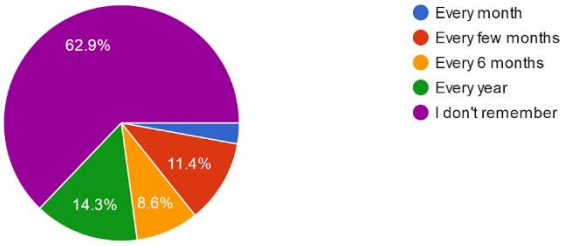
What, if any social media platforms do you use?

35 responses



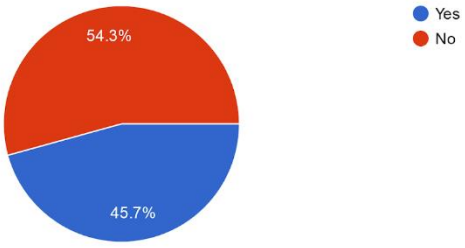
How often do you change your password

35 responses



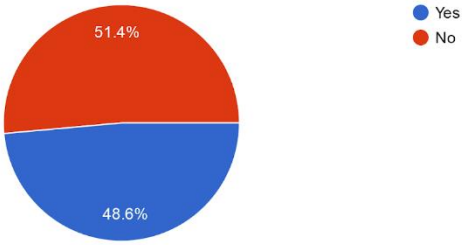
Do you share any accounts with anyone?

35 responses



Are you studying currently?

35 responses



.